JC11 Rec'd PCT/PTO 09 MAR 2001

FORM PTO-1390 (REV. 5-93)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
2345/147

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/786819

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED:
PCT/EP99/06371	**30 August 1999 (30.08.99)**	**9 September 1998 (09.09.98)**

TITLE OF INVENTION
METHOD FOR VERIFYING ACCESS AUTHORIZATION FOR VOICE TELEPHONY IN A FIXED NETWORK LINE OR MOBILE TELEPHONE LINE AS WELL AS A COMMUNICATIONS NETWORK

APPLICANT(S) FOR DO/EO/US
Axel SUSEN and Stefan BROCK

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) UNSIGNED.
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report, Preliminary Examination Report, and PCT/RO/101.

Express Mail No.: EL302703433

1602 Rec'd PCT/PTO 09 MAR 2001

U.S. APPLICATION NO (if known, see 37 CFR 1.5) 09/786819	INTERNATIONAL APPLICATION NO PCT/EP99/06371	ATTORNEY'S DOCKET NUMBER 2345/147

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)): Search Report has been prepared by the EPO or JPO $860.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) . . . $690.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $710.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1,000.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	15 - 20 =	0	X $18.00	$0	
Independent Claims	3 - 3 =	0	X $80.00	$0	
Multiple dependent claim(s) (if applicable)			+ $270.00	$	
TOTAL OF ABOVE CALCULATIONS =				$860	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$860	
Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$860	
Fee for recording the enclosed assignment (37 CFR 1 21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$860	
				Amount to be: refunded	$
				charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $860.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

By Reg. No 35,952

SIGNATURE

SEND ALL CORRESPONDENCE TO:
Kenyon & Kenyon
One Broadway
New York, New York 10004
Telephone No. (212)425-7200
Facsimile No. (212)425-5288

Richard L. Mayer, Reg. No. 22,490
NAME

3/9/01
DATE

26646
PATENT TRADEMARK OFFICE

09/786819 09/786819
JC02 Rec'd PCT/PTO 0 9 MAR 2001

[2345/147]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s)	:	Axel SUSEN et al.
Serial No.	:	To Be Assigned
Filed	:	Herewith
For	:	METHOD FOR VERIFYING ACCESS AUTHORIZATION FOR VOICE TELEPHONY IN A FIXED NETWORK LINE OR MOBILE TELEPHONE LINE AS WELL AS A COMMUNICATIONS NETWORK
Examiner	:	To Be Assigned
Art Unit	:	To Be Assigned

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

SIR:

Kindly amend the above-identified application before examination, as set forth below.

IN THE TITLE:

Please replace the title with the following:

--METHOD FOR VERIFYING ACCESS AUTHORIZATION FOR VOICE TELEPHONY IN A FIXED NETWORK LINE OR MOBILE TELEPHONE LINE AS WELL AS A COMMUNICATIONS NETWORK--.

IN THE SPECIFICATION:

Please amend the specification, including abstract, pursuant to the attached substitute specification. Also attached is a red-lined copy of the

 EL302703 433

specification, indicating deleted and added sections. No new matter has been added.

IN THE CLAIMS:

Please cancel original claims 1-15 and revised claims 1-14 (filed in the underlying PCT application) without prejudice.

Please add the following new claims:

16. (New) A method of verifying access authorization for voice telephony for a fixed network line or a mobile telephone line, comprising:

providing a first voice signal of a first subscriber placing a telephone call;

analyzing the first voice signal via a voice recognition algorithm when one of (a) before a communication connection between the first subscriber and a second subscriber is established and (b) after the communication connection between the first subscriber and the second subscriber is established, and if the analyzing begins after the communication connection between the first subscriber and the second subscriber is established then the first voice signal and a second voice signal of the second subscriber continue to be relayed;

comparing the first voice signal with a voice reference data record to determine an identity of the first subscriber;

determining if the first voice signal is in the voice reference data record and if the first voice signal is not in the voice reference data record then at least one communication effect occurs, the at least one communication effect including not establishing the communication connection, automatically interrupting the communication connection and generating an alarm in the communication connection;

recording the first voice signal before and after a communication connection to the second subscriber is established;

assigning the voice reference data record to the fixed network line or the mobile telephone line; and

recording a voice sample of the first subscriber and the second subscriber at regular time intervals during the communication connection and checking the first and second voice signals with the voice reference data record.

17. (New) The method of claim 16, wherein the voice reference data record contains reference voice samples corresponding to at least one specific spoken word, and the voice recognition algorithm analyzes a recorded voice signal with the reference voice samples for a match within a determined tolerance range.

18. (New) The method of claim 16, wherein the voice reference data record corresponds to a reference speech pattern independent of semantic content and characteristic of a person, and the voice recognition algorithm creates a corresponding speech pattern from the recorded voice signal by statistically analyzing the recorded voice signal, the corresponding speech pattern being compared with the reference speech pattern.

19. (New) The method of claim 18, wherein the reference speech pattern is characteristic of a specific frequency distribution of spoken language by the person.

20. (New) The method of claim 16, wherein the reference data record is assigned to a PBX line of a private branch exchange.

21. (New) The method of claim 16, wherein the recorded voice signal is recorded during a predetermined time interval after the initiation of the communication connection, and the recording is terminated at a conclusion of the communication connection.

22. (New) The method of claim 16, wherein the recorded voice signal is stored in an intermediate memory, and further comprising erasing the recorded voice signal stored in the intermediate memory if the recorded voice signal is determined as matched with the reference data record, and continuing to store the recorded voice

signal if the recorded voice signal is determined as not-matched with the reference data record.

23. (New) The method of claim 16, wherein the method is actuated only at at least one of a predetermined time of day, a predetermined time of month, and a predetermined call destination, and the communication connection cannot be established during at least one of a time outside the predetermined time of day, a time outside of the predetermined time of month, and a call destination outside of the predetermined call destination.

24. (New) The method of claim 16, further comprising assigning a predetermined authorization code to the fixed network line or the mobile telephone line and if the first subscriber enters the predetermined authorization code before the communication connection is established then the method is not actuated, the first subscriber entering the predetermined authorization code by at least one of an acoustic signal and via a key pad.

25. (New) The method of claim 16, further comprising recording an amount of an attempt of unauthorized access of the fixed network line or the mobile telephone line and blocking the access of the fixed network line or the mobile telephone line if the amount of the attempt of unauthorized access is equal to or larger than a predetermined maximum attempt value within a predetermined time interval.

26. (New) A communication network comprising:

a calling line and a called line, the calling line and the called line being at least one of a fixed network line and a mobile telephony line;

a technical means for establishing a communication connection between the calling line and the called line;

an accessing means for accessing a data line via which a first voice signal is at least partially transmitted between the calling line and the called line, the accessing means being configured to record the first voice signal transmitted by the calling line;

a memory in which a reference data record is stored, the reference data record containing a reference voice sample of a person having access authorization to the calling line;

a control unit having a voice recognition unit configured to access the memory for the stored reference data record, analyze the recorded first voice signal using voice recognition algorithms, and determine if the first voice signal belongs to the person having access authorization to the calling line by comparing the recorded first voice signal with the stored reference data record, the control unit configured to initiate production of an interrupt signal to interrupt the communication connection if the voice recognition unit determines that the first voice signal does not belong to the person having access authorization to the calling line;

if the voice recognition unit determines that the first voice signal does belong to the person having access authorization to the calling line then the accessing means records a voice sample at regular time intervals during the entire communication connection, the voice recognition unit determining whether the voice sample belongs to a person having access authorization to at least one of the calling line and the called line.

27. (New) The communication network of claim 26, wherein the control unit and the memory are arranged within one of a telephone system and a private branch exchange, and the stored reference data record corresponds to at least one of a reference voice sample and a reference speech pattern of the person having access authorization to at least one of the calling line and the called line.

28. (New) The communication network of claim 26, further comprising an exchange, the control unit and the memory being assigned to the exchange, the reference data record of the calling line is assigned to the exchange and stored in the memory, and the control unit causes the exchange to do at least one of generate a signal interrupting the communication connection and generate an alarm if the voice sample cannot be matched with the stored reference data record.

29. (New) The communication network of claim 26, further comprising a Service Control Point (SCP) of an intelligent network, the control unit and the memory being assigned to the Service Control Point, the control unit causing the Service Control Point to do at least one of generate a signal interrupting the communication connection and generate an alarm if the voice sample cannot be matched with the stored reference data record.

30. (New) A mobile terminal for telecommunications, comprising:

an accessing means for accessing a data line via which a voice signal is transmitted in electronic form and for recording the voice signal and an entered signal;

at least one memory in which an at least one reference data record is stored, the at least one reference data record being assigned to a group of persons having an access authorization;

at least one control unit having a voice recognition unit configured to access the at least one memory for the at least one reference data record and to analyze the recorded voice signal via a voice recognition algorithm and to determine the access authorization by comparing the recorded voice signal with the at least one reference data record, the at least one control unit effecting at least one of initiating production of an interrupt signal to interrupt the communication connection and initiating a shut-off of the terminal if the recorded voice signal does not match with the at least one of the at least one reference data record; and

a sampling means for recording voice samples at regular time intervals during the entire communication connection, the at least one control unit determining whether the voice sample belongs to a person of the group of persons having access authorization.

REMARKS

This Preliminary Amendment cancels, without prejudice, original claims 1-15 and the revised claims 1-14 in the underlying PCT Application No. PCT/EP99/06371, and adds new claims 16-30. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

The amendments to the specification and abstract reflected in the substitute specification are to conform the specification and abstract to U.S. Patent and Trademark Office rules, and do not introduce new matter into the application.

The underlying PCT Application No. PCT/EP99/06371 includes an International Search Report, dated December 20, 1999, a copy of which is included. The Search Report includes a list of documents that were considered by the Examiner in the underlying PCT application.

The underlying PCT Application No. PCT/EP99/06371 also includes an International Preliminary Examination Report, dated December 13, 2000, a copy of which is included, including a translation.

Applicants assert that the present invention is new, non-obvious, and useful. Prompt consideration and allowance of the claims are respectfully requested.

Respectfully Submitted,

KENYON & KENYON

Dated: 3/9/01

By: [signature] Reg. No. 35,952

By: [signature]
Richard L. Mayer
Reg. No. 22,490

One Broadway
New York, NY 10004
(212) 425-7200

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) **Internationale Patentklassifikation** 7 : **G10L 17/00, H04M 3/38**

A1

(11) **Internationale Veröffentlichungsnummer:** **WO 00/14730**

(43) **Internationales Veröffentlichungsdatum:** 16. März 2000 (16.03.00)

(21) **Internationales Aktenzeichen:** PCT/EP99/06371

(22) **Internationales Anmeldedatum:** 30. August 1999 (30.08.99)

(30) **Prioritätsdaten:**
198 41 166.9 9. September 1998 (09.09.98) DE

(71) **Anmelder** *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) **Erfinder; und**
(75) **Erfinder/Anmelder** *(nur für US)*: SUSEN, Axel [DE/DE]; Heinrichsallee 66, D–52062 Aachen (DE). BROCK, Stefan [DE/DE]; Hennefer Strasse 6b, D–53737 Sankt Augustin (DE).

(74) **Gemeinsamer Vertreter:** DEUTSCHE TELEKOM AG; Rechtsabteilung (Patente), PA1, D–64307 Darmstadt (DE).

(81) **Bestimmungsstaaten:** US, europaisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

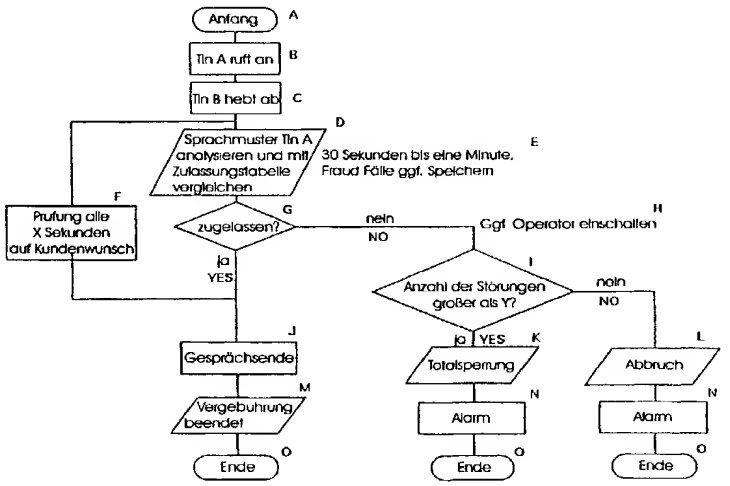
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) **Title:** METHOD FOR CHECKING ACCESS AUTHORISATION FOR VOICE TELEPHONY AT A FIXED NETWORK OR MOBILE TELEPHONE CONNECTION AND CORRESPONDING COMMUNICATIONS NETWORK

(54) **Bezeichnung:** VERFAHREN ZUR KONTROLLE DER ZUGANGSBERECHTIGUNG FÜR DIE SPRACHTELEFONIE AN EINEM FESTNETZ– ODER MOBILTELEFONANSCHLUSS SOWIE KOMMUNIKATIONSNETZ

(57) **Abstract**

The invention relates to a method for checking access authorisation at a fixed network or mobile telephone connection and to a communications network which checks access authorisation in this way. According to the invention, access authorisation is checked by analysis of a voice signal provided by the subscriber before or during an ongoing conversation. According to one variant, the voice signal is given in the form of a password before the connection is established. According to another variant, the voice and the subscriber are identified by analysing the voice signals which are also transmitted to the call recipient, so that the access check can be carried out in a concealed manner without hindering the flow of the conversation.



A. .START
B. .SUBSCRIBER A CALLS
C. SUBSCRIBER B PICKS UP
D .ANALYSE SUBSCRIBER A AND COMPARE WITH AUTHORISATION TABLE
E. 30 SECONDS TO A MINUTE, STORE CASES OF FRAUD, OPTIONALLY
F...CHECK EVERY X SECONDS ACC. TO CUSTOMER'S WISHES
G AUTHORISED ?
H...OPTIONALLY, ACTIVATE OPERATOR
I NUMBER OF FAILURES GREATER THAN Y ?
J .CONVERSATION TERMINATED
K. BLOCK
L...DISCONNECTION
M. BILLING TERMINATED
N .ALARM
O...END

(57) **Zusammenfassung**

Die Erfindung betrifft ein Verfahren zur Kontrolle der Zugangsberechtigung für die Sprachtelefonie an einem Festnetz– oder Mobiltelefonanschluß sowie ein Kommunikationsnetz mit einer derartigen Zugangsberechtigungskontrolle. Die Zugangsberechtigung wird erfindungsgemäß durch Analyse eines Sprachsignals, welches vor oder während eines laufenden Gesprachs vom rufenden Teilnehmer eingegeben wurde, kontrolliert. In einer Variante wird das Sprachsignal als Paßwort vor dem Verbindungsaufbau eingegeben, in einer anderen Variante werden zur Spracherkennung und Teilnehmeridentifizierung diejenigen Sprachsignale untersucht, welche auch an den Kommunikationspartner übertragen werden, so daß eine verborgene, den normalen Gesprächsablauf nicht behindernde Zugangskontrolle möglich ist.

09/786819
JC02 Rec'd PCT/PTO 0 9 MAR 2001

[2345/147]

METHOD FOR VERIFYING ACCESS AUTHORIZATION FOR VOICE TELEPHONY IN A FIXED NETWORK LINE OR MOBILE TELEPHONE LINE AS WELL AS A COMMUNICATIONS NETWORK

Technical Field

The invention relates to a method for verifying access authorization for voice telephony in a fixed network line or mobile telephone line as well as a communications network having such access authorization verification.

Background of the Invention

In the case of private branch exchanges (PBXs) for telecommunications having a large number of extension stations used by different persons, but also in the case of mobile terminals, in other words, cell phones, there exists the problem of abuse by unauthorized third parties or by unauthorized employees of a company. For example, personal conversations are frequently held via PBX lines of large corporations at the employer's expense. Moreover, when telephone calls are made from a stolen or lost mobile telephone, the account of the lawful owner is always charged without the owner being able to directly prevent this.

To prevent unauthorized use in private branch exchanges, methods are known in which the user of a terminal must enter an access code to be able to make an interoffice call and/or to dial specific outside numbers. In these methods, the subscriber enters a personal access code (PIN) via the keypad of the terminal, the access code being evaluated by the private branch exchange and

EL302703433

compared with a table of authorized names. This method also makes it possible to allocate the incurred charges to specific individuals. Once the subscriber's authorization has been established in this manner, the corresponding PBX line is enabled to establish an interoffice or long-distance connection.

However, due to the additional time required, this method of entering a code before each call is very cumbersome and is not practicable for PBX lines from which many calls are made regularly, e.g., a secretary's office or a senior executive's office. For that reason, such lines are frequently exempted from the access verification so that any person can call from them at any time and the problem of unauthorized use persists.

An additional known method is to detect unauthorized use after the fact by analyzing the call durations, the direction, and the subscriber called or the number called. For this purpose, the private branch exchange logs the calls made, the call destinations, call duration, and the associated PBX line. A similar verification takes place in the network management system of a public switched telephone network. For example, all calls lasting longer than a predetermined duration are checked for the call destination later or during the connection. An unauthorized use can be detected if the call destination cannot be assigned to a predetermined group of telephone numbers, which, for example, are assigned to the company's customers. Individual PBX lines such as those of senior executives can be exempted from checking for unauthorized use in this case also.

However, even with this type of checking for unauthorized use, only line-specific determination of an unauthorized

use is possible. Those cases in which the same person improperly uses different terminals without authorization cannot be detected. Moreover, the unauthorized use can only be detected after the fact; an unauthorized call cannot be prevented.

U.S. Patent 5,623,539 relates to a device and a method for monitoring a telephone connection for unauthorized use. For this purpose, voice samples of all of the persons who are authorized to use the telephone connection are stored. During a conversation conducted over the telephone connection, the transmitted voice data is tapped and broken down via suitable means into individual voice samples, each of the thus-obtained voice samples corresponding to the voice of one of the conversation participants. These voice samples taken from the telephone conversation are compared to the stored voice samples. The telephone connection is only accepted as authorized when a sufficient match between at least one of the stored voice samples and at least one of the voice samples obtained from the telephone conversation is determined.

U.S. Patent 5,093,855 relates to a method and a device for speaker recognition in a telephone switching exchange, where tapped speech samples are supplied via the telephone line to the exchange, where they are compared to previously stored speech samples. If the speaker is recognized, a first signal is emitted, otherwise, a second signal is emitted.

The publication "Speaker Identity Verification over Telephone Lines: Where we are and where we are going" by T.C. Feustel and G.A. Velius, International Carenaham Conference, Zurich 1989, addresses voice recognition and

the security, e.g., against unauthorized telephone use, that it can provide. In this context, the possibility to increase security by combining voice recognition and the use of passwords or PINs is also mentioned.

Technical Object

The object of the present invention is therefore to provide a method for verifying access authorization for voice telephony that does not hamper the normal use of telephones and permits direct detection of attempts at unauthorized use and prevents them if necessary.

Summary of the Invention

The objective is achieved by a method for verifying access authorization for voice telephony in a fixed network or mobile telephone line by voice recognition according to Claim 1. Advantageous further developments of the invention are the object of the dependent claims.

According to the present invention, voice signals of the subscriber placing the call are recorded before or after the communication connection to the subscriber being called is set up. For example, the subscriber can be automatically prompted to acoustically provide a password after dialing the outside number, but before the connection is established. Alternatively, the voice signals are recorded during the course of the call, the voice signals of the subscriber placing the call being relayed concurrently to the subscriber called so that the communication is not disturbed. In both cases, the voice signal of the subscriber placing the call is analyzed by voice recognition algorithms and compared with a reference data record or several reference data records

for purposes of assignment. The reference data record(s) is/are assigned to the fixed network line or mobile telephone line in an unambiguous manner; in particular, they define the group of persons having authorized access. According to the present invention, the communication connection is automatically disconnected or is not established and/or an alarm is triggered, if the recorded voice sample cannot be assigned to any reference data record. Otherwise, the communication connection is maintained or established in the customary manner.

Preferably, voice recognition takes place after the start of the communication connection online, i.e., directly during the communication connection. As with line tapping by police or intelligence services, the voice signals of the subscriber placing the call are tapped from the data line and supplied to a voice recognition unit, which analyzes them online. The voice data is transmitted concurrently to the person called. If the voice recognition unit is able to make an assignment to a reference data record, the analysis of the voice signal is terminated, and the data processing capacity of the voice recognition unit is available for identifying additional callers.

As an alternative to voice recognition during the connection, the speaker can be assigned to a billing account before the connection is established as part of an authentication procedure that the speaker must undergo. In this case, the telephone user is requested to provide a voice sample, and the connection is only established once the voice sample has been identified and the speaker is identified as authorized.

In addition to online voice recognition, the voice signal

of the subscriber placing the call can also be recorded and stored in intermediate memory as a voice sample. The stored voice sample is then analyzed during or after the communication connection.

The method according to the present invention has the particular advantage that it is not necessary to perform the cumbersome action of entering a password manually before the communication connection is established, but rather access is established or maintained by voice control. When access authorization is verified after the connection has been established, the process takes place concurrently with the normal flow of the call; the participants do not notice the access verification, but rather they are able to talk over the telephone in the normal manner, thus saving time. The same voice signals that are transmitted to the person called are analyzed for voice recognition and subscriber identification. This does not interfere with the transmission of voice signals between the conversation participants. Thus, in principle, any connection can be monitored for unauthorized use without interfering with the normal flow of telephone conversation by additionally entering access codes.

Several possibilities for voice recognition are known and can be used to implement the present invention. There are voice recognition algorithms for recognizing semantic content of speech that compare an actual voice sample with an already stored voice sample corresponding to a specific spoken word. In this context, the stored voice sample corresponds, for example, to a spoken word whose text representation is also stored. By determining a correspondence between the actual and the stored voice sample, it is possible to assign a textual

representation, e.g., in the form of an ASCII representation, to the actual voice input, thus in principle making it possible to recognize the content of a voice message. Such voice recognition units are used, for example, for the voice control of computers and the like.

Typically, the future user inputs the stored voice sample during a training phase. The typical result is that, even in this case, only the actual voice input of this user can be reliably recognized by the voice recognition, since even voice samples of different users that have the same semantic content vary due to individual speech patterns.

This principle can also be used in a refinement of the present invention to verify access authorization for a telephone line. In this connection, the reference data records are reference voice samples corresponding to specific words spoken by one person, e.g., typical greetings, the first or last name of a person having authorized access or other expressions which frequently occur in a telephone conversation. These voice samples are recorded in a training phase and stored in digital form in a memory as a reference data record. In order to implement the method, the voice recognition algorithms analyze the recorded voice data for the occurrence of fragments, i.e., individual words or expressions that match the reference voice sample within a specified tolerance range. In this connection, it is not the semantic content of the reference or of the actual voice signal that is of significance, but rather the individual speech pattern of the authorized and the calling persons which is expressed in a specific characteristic pattern of the reference voice sample.

For this reason, another preferred embodiment does not provide for the use of an actual word recognition system like the one described above, but rather for the analysis of the input voice signals for speech patterns that are characteristic of the user regardless of their semantic content. The specific intonation, voice register, dialect, and the like, which cause the voice of a person to appear nearly unique to the human ear, are manifested in characteristic features of a voice sample taken from this person, e.g., a specific frequency distribution, which can be used to identify this person by electronic means. Therefore, according to the present invention, reference speech patterns, e.g., frequency patterns or amplitude patterns, which are characteristic of one person, are stored as reference data records. For example, they are obtained by statistical analysis of a voice sample using a corresponding voice recognition algorithm. To identify the actual voice sample recorded during a call, the voice recognition algorithms then create a corresponding speech pattern by statistically analyzing the sample. In this connection, statistical analysis primarily refers to a frequency analysis in which the tone and voice register of the speaker can be identified; dynamic analysis refers to the dynamics of the voice signal, i.e., the amplitude characteristic and, accordingly, a specific intonation. Both methods are suitable for identifying a speaker. This speech pattern is then compared with the reference speech patterns. It is determined whether the characteristic features of both patterns agree. In creating the reference speech pattern from a reference voice sample, it is important that the same voice recognition algorithm be used with which the actual voice sample is analyzed.

The advantage of this variant is that the analysis of the

individual speech patterns makes a significantly more accurate identification of the speaking person possible than the search for specific words which, although individually characterized, may not always be reliably detectable due to the shortness of the words. The first variant is particularly suited for access verification by entering a specific spoken password, while the second variant is particularly suited for covertly verifying the access authorization during an ongoing call.

The reference data records correspond to the group of authorized persons, e.g., all the employees of a company who must make telephone calls as part of their work activity. The reference data records are stored, for example, in a table of authorized names. In this context, one person can be authorized only for selected telephone numbers or types of connections, or authorization can change as a function of the time of day.

The method according to the present invention can advantageously prevent the use of terminals for the placement of toll calls by persons not belonging to this authorized group, while any authorized person can place calls from any PBX line of the company.

In an additional advantageous refinement of the present invention, the access authorization is further differentiated according to PBX lines. The reference data record or reference data records are unambiguously assigned to a PBX line of a private branch exchange. The reference data record or reference data records, in turn, define the group of authorized persons, in this case for a single PBX line. This makes it possible to prevent persons authorized per se from placing telephone calls from other terminals. This is important in the event that

individual lines are cleared for interoffice calls but not for long distance calls, while this limitation does not exist for other PBX lines.

In the event of an access verification during the connection, the voice signals are tapped during a predetermined time interval, e.g., 30 to 60 seconds, the recording starting in particular immediately after the connection is established. The voice sample is already analyzed during the tapping or at the end of the time interval.

For reasons of data security and privacy, the recorded and possibly buffered voice sample is erased after the voice recognition is completed, if it was possible to assign the sample to a reference data record. However, in the case of unauthorized use, i.e., no automatic assignment can be made to a reference data record and, accordingly, to an authorized person, the voice data preferably remains stored. It can then be used to identify the speaker.

In order to keep the expense for verifying access authorization as low as possible, it is advantageous if the method is implemented only at certain times of the day and/or week and/or only via specific call destinations, e.g., only for long-distance connections. The fixed network or mobile telephone line in question, or individual PBX lines of a fixed network line are then completely blocked or completely cleared for connections outside of these time periods or for other call destinations.

Moreover, it is provided that the access verification by voice recognition is not implemented if, before a

connection is established, the user enters a key combination, e.g., a PIN code or an acoustic signal, e.g., a sequence of MFC signals, and has his authorization verified via this access code.

An additional advantageous refinement of the present invention provides that the number of unauthorized access attempts is recorded and the line is blocked if more than a predetermined number of such attempts is detected within a predetermined time interval, e.g., one day or one hour. In addition, an alarm can first be triggered via the network management system, and an operator can be switched in.

Furthermore, the objective is achieved by a communication network having a plurality of fixed network lines or mobile telephone lines, as well as technical means for establishing a communication connection between two or more lines of the same or of a different communication network, including:

a) means that are capable of accessing a data line via which voice signals are at least partially transmitted from the calling line to the called line, and that are capable of recording a voice signal transmitted by the calling line;

b) at least one memory in which reference data records are stored which are assigned to a group of persons having access authorization;

c) at least one control unit having a voice recognition unit which is capable of accessing the memory for the reference data records, analyzing the tapped voice signal via voice recognition algorithms, and determining the access authorization of the subscriber placing the call by comparison with the reference data

records, the control unit initiating the production of a signal to disconnect the connection if the voice signal cannot be assigned to any of the reference data records, characterized in that voice samples are recorded at regular time intervals during the entire communication connection, and the speaker's authorization is checked at regular time intervals.

In this context, a communication network is understood to be the totality of all lines including the exchanges or conversion stations and possibly data lines and other intelligent switching and transmission devices. The elements involved in the present invention can, however, be arranged in only a small part of the network, e.g., in a private branch exchange. The communication network according to the present invention advantageously makes it possible to verify the access authorization of users of individual lines and accordingly to implement the method according to the invention.

In order to be able to utilize the voice signals in a detected case of abuse, to identify the unauthorized caller or for offline voice analysis, the communication network preferably has at least one memory in which the recorded voice signals are stored in intermediate memory as voice samples.

According to the present invention, the verification of access authorization within the communication network can take place at various points within the network. If the access authorization of users of a private branch exchange is to be verified, the control unit and the reference data memory or possibly the voice sample memory are preferably arranged within the private branch

exchange. The control unit is, for example, part of a data processing system that logs the connections made by the individual PBX lines, blocks individual PBX lines on a time-dependent basis or for specific call destinations, and possibly requests a PIN code.

Alternatively, the control unit and the corresponding memory locations are able to be located outside the customer area in an exchange in the actual telephone network. In this case, the reference data of the lines assigned to the exchange is stored in the reference data memory. Preferably, the reference data is stored in a line-specific manner, so that an authorized group of persons is defined for each line and is checked by the exchange. If the control unit is unable to assign the voice sample to any of the reference data records, it causes the exchange to generate a signal disconnecting the connection. In this manner, a common control unit can be used to centrally verify the access authorization of users of a plurality of lines in the exchange without requiring a modification of the lines on the customer side.

Access verification can be further centralized by assigning the control unit and the corresponding memory to an SCP (Service Control Point) of an intelligent network and by the control unit causing the SCP to generate a signal interrupting the connection if the voice sample cannot be assigned to any of the reference data records. The so-called intelligent network is an open communications network, which is built on the traditional telephone network and makes various telephone services having new features possible, for example, toll-free calling using specific numbers or reaching various offices of a corporation using a dial number that is

identical over a larger region. The central computer containing the required switching information is known as the SCP. The transition from a telephone network of one network provider to that of a different network provider is also accomplished using structures similar to an IN.

In addition, the method according to the present invention can also be advantageously used to check the authorization of a mobile terminal user.

For this purpose, a mobile terminal for telecommunications is proposed, including:

a) means that are capable of accessing a data line, via which voice signals are transmitted in electronic form, and of recording an entered signal and a voice signal;

b) at least one memory in which at least one or more reference data records are stored which are assigned to a group of persons having access authorization;

c) at least one control unit having a voice recognition unit which is capable of accessing the memory for the reference data records, analyzing the tapped voice signal via voice recognition algorithms, and of determining the access authorization of the subscriber placing the call by comparison with the reference data records, the control unit initiating the production of a signal to disconnect the connection or causing the terminal to shut off if the voice signal cannot be assigned to any of the reference data records,

characterized in that voice samples are recorded at regular time intervals during the entire communication

connection, and the speaker's authorization is checked at regular time intervals.

The reference data record(s) is/are preferably stored on the chip of a mobile telephone card. The owner of the mobile telephone preferably provided the voice sample necessary for this purpose when purchasing the mobile telephone card. Therefore, a lost mobile telephone is, in principle, operable, but the mobile telephone card is only operable as a function of the correct speech pattern. This can prevent calls from continuing to be made on a lost mobile telephone at the owner's expense.

Brief description of the drawing in which:

Figure 1	schematically shows the sequence of operations of the method according to the present invention;
Figure 2	shows an additional flowchart of the method according to the present invention;
Figures 3-5	show examples of communication networks for implementing the method according to the present invention.

The sequence of operations of the method according to the present invention is schematically shown in Figure 1. At the start of the method, subscriber A calls a destination number. The connection is established as soon as subscriber B answers. Typically, both subscribers begin to speak. The voice signals of subscriber A are automatically tapped and analyzed, the analysis lasting a predetermined time span, approximately 30 seconds to one minute. A interoffice trunk, via which the voice signals between both users are transmitted, is accessed without interfering with the transmitted signal, so that the

access verification does not affect the conversation.

The voice signal of subscriber A is analyzed, i.e., compressed by voice recognition algorithms, the thus-produced speech pattern being compared with reference data records stored in a table of authorized names. If the actual voice signal can be assigned to one of the reference data records, then the subscriber is considered to be authorized and entitled to call. In this context, the table of authorized persons can refer specifically to the line as a whole or to a PBX line and/or it may be time-dependent.

If subscriber A is approved, then the connection is maintained until the end of the call. In the simplest case, no additional check is made. To further increase security against abuse, the process is repeated at regular time intervals, i.e., the voice signal of subscriber A is analyzed again.

If the subscriber is identified as unauthorized, because his voice signal cannot be assigned to an entry in the table of authorized persons, the connection is interrupted in the simplest case by generating a interrupting signal or by briefly deactivating the terminal. In principle, it is possible to establish a new connection immediately after the connection is terminated.

To counteract persistent attempts at unauthorized use, it is also possible to record the number of attempts at unauthorized use within a specific time interval and to set a critical value for the maximum number to be tolerated. If the number of attempts at unauthorized use exceeds this value, a total block of the line is

automatically initiated. The line can then only be enabled again after a specific waiting period or by the entering an enabling code. In addition, as in the case of a normal termination due to unauthorized use, an alarm signal can be produced at the telephone itself or at a PBX operator desk.

Figure 2 shows an additional flowchart of the method according to the present invention. Before the method is initiated, all users of the telephone line to be protected against abuse enter voice samples into the system. The voice recognition unit or a speech pattern recognition system extracts the subscribers' speech patterns and stores them, compressed by a voice recognition algorithm, in memory as reference data. The reference speech patterns are, thus, available for online recognition at the facilities of the network provider, in a private branch exchange, or on the calling card of a mobile telephone.

The process begins once a caller initiates a call from a telephone, the telephone connection is established by the network provider, and the telephone conversation is started. At the same time as the telephone call, the speech pattern recognition is initiated to determine the speech pattern of the caller. This speech pattern determined for the caller from the telephone call is compared with the reference stored for this line or on the calling card of a mobile telephone.

If a speech pattern is recognized, i.e., the actual voice signal matches a reference, the speech pattern recognition for this connection is discontinued, and the computer capacity can be used to analyze other calls.

If no speech pattern is recognized, the call is interrupted to protect the customer from financial loss. When a mobile telephone is used with a calling card, the call is always terminated. If necessary, the customer can be provided with a log of the attempt at unauthorized use in order to identify the person using the telephone without authorization.

Figures 3 through 5 show three possibilities for implementing the method according to the present invention in a communications network.

For this purpose, Figure 3A shows a private branch exchange (PBX), which is connected to a public switched telephone network. The private branch exchange (PBX) has a plurality of extension stations, of which three are shown here. The access authorization of the users of the individual extension stations is to be monitored according to the present invention. For this purpose, an IP (intelligent peripheral) is assigned to the private branch exchange (PBX), the IP being capable of accessing the telephone line via which signals are transmitted from one extension station to an additional line outside the private branch exchange, and of recording and storing the signals entered by the extension station user. In addition, the IP has a voice recognition unit that is capable of analyzing the recorded voice signal and comparing it with previously stored reference data records. In addition, the IP is also capable of accessing the reference data record memory. In this case, either specific reference data records are assigned to each extension station, the reference data records being assigned to the users of this extension station, or the table of authorized persons contains all potential users of the entire private branch exchange irrespective of the

actual PBX line.

If the IP cannot match the actual voice sample to any of the reference data records, it applies a suitable control signal to induce the private branch exchange (PBX) to generate a signal interrupting the connection. As a result, the connection of a PBX line to a user in the public switched telephone network via the private branch exchange is interrupted.

Figure 3B shows an example for the implementation of person-specific assignment of charges by voice recognition in a private branch exchange.

In the private branch exchange, in the case of procedural authentication, i.e., voice recognition before a connection is established, all calls originating from the terminals connected to PBX lines (ports 22 to 28) are redirected to one port (port 21 in the illustrated example). This redirection is performed by the control unit of the private branch exchange. The relevant programs are stored, for example, in a memory module, an EEPROM in this case. A digital signal processor (DSP) having suitable voice recognition software and, optionally, voice recognition hardware is connected to port 21. If the identification is positive, it relays the signal to the private branch exchange via the customary control functions, i.e., either via the line, a V.24 interface, or another management interface. The thus-verified calls are switched from the private branch exchange (PBX) to the interexchange trunk and form an outgoing call. The billing information for person-specific cost assignment is fed directly into the billing system.

In the case of online recognition of the speaker, the call is already set up; however, as in the case of "bugging" a call, the call information is serially routed through the DSP. The DSP analyzes the speech without interfering with the transmission and relays corresponding information to the private branch exchange or the billing system.

Figure 4A shows an arrangement of control unit IP corresponding to the arrangement of Figure 3A in an exchange. A connection from the subscriber line to an additional line in the public switched telephone network is established via this exchange. Physically and organizationally, the exchange is assigned to the subscriber line; however, it is not necessarily located in its immediate vicinity. Aside from the different physical arrangement of the IP, the access verification is performed here in the same manner as described above. The difference is that no intelligent devices for voice recognition and for speech storage need to be provided on the subscriber side, since these are centrally integrated in the exchange.

Figure 4B shows an example for the implementation of access verification by voice recognition in an exchange of a telephone network.

Voice recognition system IP can be implemented in a computer, for example in the form of a plug-in module in the exchange. Calls for which the speaker is to be identified are routed from the exchange through the IP.

Voice recognition is implemented either in dialog form, i.e., an authentication procedure is executed as described above in Figure 3B, or else the voice is

recognized online. In the latter case, the speech pattern is checked during the conversation in progress and characteristics of the speech of speaking user A are compared with the stored patterns. In this case, the call is tapped, so to speak, by the IP without interfering with it.

One possible structure for the authentication procedure is a dial-in into the DSP of the IP. For this purpose, the telephone channel is routed to an input of the IP. At this point, subscriber A is asked by the software of an intelligent voice response system to state his name or his identifier. After that, he is asked for his password or his personal identification number PIN. The data is compared with the identifier stored in memory, and the speech pattern is compared with the stored patterns either using frequency spectra or speech dynamics. In the dialog form, the implementation of voice recognition is very simple, since the identifier is made up of precisely defined words, which were previously entered.

After authentication in the IP, the customer is directed to a menu that requests that he enter the desired telephone numbers. These are recorded as in conventional messaging or voice response systems, converted into pulse or MFC dialing information, and sent into the network, or they are relayed to the exchange as signals in the format of signaling system No. 7 (Common Channel Number 7, CCS7). The exchange then initiates the connection to subscriber B. The use of CCS7 signals permits faster processing and more features, namely all those implemented in CCS7 and cleared for the IP.

The information concerning the speaker, i.e., the identified reference data record, is sent as control

information to the exchange via the CCS7, and generates an alarm in the network management system. The network management system can also generate a corresponding alarm message regarding call data records, so that the billing system also receives appropriate information.

The speaker-identifying data records produced in this way are used for access verification; however, they can also be used for billing a call. The corresponding procedures are described in the flowcharts.

When recognizing continuous speech, the system preferably concentrates on the essential characteristics of the language. To be sure, key words such as "good morning, hello," etc. can be considered in the entry procedure; however, in principle, it is necessary to store speaker-specific characteristics, irrespective of which language and with whom the user is speaking. For this purpose, the algorithm can use static methods such as frequency spectrum analysis, as well as dynamic speech characteristics.

Figure 4C shows an additional example of the method according to the present invention implemented in an exchange. The subscriber unit (subscriber card) of subscriber A recognizes whether the subscriber has provided voice recognition for access verification. The central processing unit CPU of the exchange initiates the appropriate routing through the switching matrix, the actual switching unit. As a result, the call is not routed directly to subscriber B or to the next exchange, but rather it is first routed through an intelligent peripheral IP having a digital signal processor (DSP). The output port of the IP is routed through the switching matrix to subscriber B or to the next exchange.

All control information and, accordingly, also the result of the voice recognition are compared in the exchange having the central processing unit CPU.

The IP can also include several voice recognition units or DSPs and, thus, analyze several lines simultaneously. The information concerning the usage of the IP and concerning the analytical results is transmitted to the CPU.

Figure 5 shows the implementation of the method according to the present invention in the service control point SCP of an intelligent network.

When implemented in the IN, the voice data is routed via an ISDN channel to voice recognition unit IP, which is located at the site of the SCP. Control information, for example, whether the calling line is using voice recognition for monitoring abuse, results from the voice analysis, and the like are then exchanged between the SCP and the service switching point SSP, which is located at the site of the exchange.

Implementing the method according to the present invention in the centrally structured IN makes it possible to centrally implement voice-based abuse control over a large network area, i.e., a plurality of lines. This eliminates the need for expensive software and hardware equipment in the exchanges; only the IN must be adapted. This implementation is, therefore, suitable in particular for cases of low demand or in the introductory phase, i.e., it is not yet worthwhile to equip each exchange.

Industrial Applicability

The present invention is suitable, in particular, for operators of communication networks to increase the security of voice telephony customers against abuse. Moreover, the present invention is particularly suitable for operators of private branch exchanges where the problem of unauthorized access is encountered on a regular basis.

Claims

1. A method of verifying access authorization for voice telephony in a fixed network line or mobile telephone line, where
   - before or after the communication connection to the subscriber being called is established, voice signals of the subscriber placing the call are analyzed via voice recognition algorithms and compared with a reference data record or several reference data records for purposes of assignment, the voice signals of the subscriber placing the call being relayed to the subscriber being called if the communication connection already exists; and
   - if the voice signals cannot be assigned to a reference data record, the communication connection is not established or is automatically interrupted, and/or an alarm signal is generated,

   characterized in that
   a) voice signals of the subscriber placing the call are recorded before or after the communication connection to the subscriber being called is established;
   b) the reference data record(s) is/are assigned to the fixed network line or mobile telephone line in an unambiguous manner; and
   c) voice samples are recorded at regular time intervals during the entire communication connection, and the speaker's authorization is checked at regular time intervals.

2. The method as recited in Claim 1, characterized in that the reference data records are reference voice

samples corresponding to specific words spoken by a person, and the voice recognition algorithms analyze the recorded voice sample for the occurrence of parts that match the reference voice sample within a specified tolerance range.

3. The method as recited in Claim 1 or 2, characterized in that the reference data records correspond to reference speech patterns which are independent of semantic content and are characteristic of one person, e.g., of a specific frequency distribution of spoken language, and in that the voice recognition algorithms create a corresponding speech pattern from the recorded voice sample by statistically analyzing the latter, the corresponding speech pattern being compared with the reference speech patterns.

4. The method as recited in Claim 1 or 2, characterized in that the reference data record(s) is/are assigned to a PBX line of a private branch exchange in an unambiguous manner.

5. The method as recited in one of the preceding claims, characterized in that
the voice sample is recorded during a predetermined time interval after the initiation of the communication connection, and the recording is terminated at the conclusion of the communication connection.

6. The method as recited in one of the preceding claims, characterized in that
the voice sample stored in intermediate memory is erased after the completion of step b) or after the

communication connection is terminated, provided the voice sample was able to be assigned to a reference data record, and otherwise continues to be stored.

7. The method as recited in one of the preceding claims, characterized in that
it is only implemented at predetermined times of the day and/or week and/or only for predetermined call destinations, the line being completely blocked or being completely cleared for connections outside of these times and/or for other call destinations.

8. The method as recited in one of the preceding claims, characterized in that
the method is not implemented if an access authorization is verified by entering a key combination (PIN code) and/or an acoustic signal before the start of the communication connection.

9. The method as recited in one of the preceding claims, characterized in that
the number of attempts at unauthorized access is recorded, and the line is blocked if more than a predetermined number of such attempts is recognized within a predetermined time interval.

10. A communication network having a plurality of fixed network lines or mobile telephony lines, as well as technical means for establishing a communication connection between two or more lines of the same or another communication network, including:
    a) means that are capable of accessing a data line via which voice signals are at least partially transmitted from the calling line to the called line, and that are capable of recording a voice

signal transmitted by the calling line;

b) at least one memory in which reference data records are stored which are assigned to a group of persons having access authorization;

c) at least one control unit having a voice recognition unit which is capable of accessing the memory for the reference data records, analyzing the tapped voice signal via voice recognition algorithms, and determining the access authorization of the subscriber placing the call by comparison with the reference data records, the control unit initiating the production of a signal to interrupt the connection if the voice signal cannot be assigned to any of the reference data records,

characterized in that voice samples are recorded at regular time intervals during the entire communication connection, and in that the speaker's authorization is checked at regular time intervals.

11. The communication network as recited in Claim 10, characterized in that the control unit and memory are arranged within a telephone system, a private branch exchange in particular, the stored reference data records corresponding to reference voice samples or reference speech patterns of individual extension station users having access authorization.

12. The communication network as recited in Claim 10, characterized in that the control unit and memory are assigned to an exchange, the reference data of the lines assigned to the exchange being stored in the memory, and in that the control unit causes the exchange to generate a signal interrupting the connection, or an alarm if the voice signal cannot

be assigned to any of the reference data records.

13. The communication network as recited in Claim 10, characterized in that the control unit and memory are assigned to an SCP (Service Control Point) of an intelligent network, and the control unit causes the SCP to generate a signal interrupting the connection, or an alarm if the voice sample cannot be assigned to any of the reference data records.

14. A mobile terminal for telecommunications, including:
    a) means that are capable of accessing a data line via which voice signals are transmitted in electronic form and of recording an entered signal and a voice signal;
    b) at least one memory in which at least one or more reference data records are stored which are assigned to a group of persons having access authorization;
    c) at least one control unit having a voice recognition unit which is capable of accessing the memory for the reference data records, analyzing the tapped voice signal via voice recognition algorithms, and of determining the access authorization of the subscriber placing the call by comparison with the reference data records, the control unit initiating the production of a signal to interrupt the connection or causing the terminal to shut off if the voice signal cannot be assigned to any of the reference data records,

characterized in that voice samples are recorded at regular time intervals during the entire communication connection, and the speaker's authorization is checked at regular time intervals.

09786819 09/786819
JC02 Rec'd PCT/PTO 0 9 MAR 2001

[2345/147]

METHOD FOR VERIFYING ACCESS AUTHORIZATION FOR VOICE TELEPHONY IN A FIXED NETWORK LINE OR MOBILE TELEPHONE LINE AS WELL AS A COMMUNICATIONS NETWORK

Field of the Invention

The present invention relates to a method for verifying access authorization for voice telephony in a fixed network line or mobile telephone line as well as a communications network having such access authorization verification.

Background of the Invention

In the case of private branch exchanges (PBXs) for telecommunications having a large number of extension stations used by different persons, but also in the case of mobile terminals such as cell phones, there exists the problem of abuse by unauthorized third parties or by unauthorized employees of a company. For example, personal conversations are frequently held via PBX lines of large corporations at the employer's expense. Moreover, when telephone calls are made from a stolen or lost mobile telephone, the account of the lawful owner is always charged without the owner being able to directly prevent this.

To prevent unauthorized use in private branch exchanges, methods are known in which the user of a terminal must enter an access code to be able to make an interoffice call and/or to dial specific outside numbers. In these methods, the subscriber enters a personal access code (PIN) via the keypad of the terminal, the access code being evaluated by the private branch exchange and compared with a table of authorized names. This method

also makes it possible to allocate the incurred charges to specific individuals. Once the subscriber's authorization has been established in this manner, the corresponding PBX line is enabled to establish an interoffice or long-distance connection.

However, due to the additional time required, this method of entering a code before each call is very cumbersome and is not practical for PBX lines from which many calls are made regularly, e.g., a secretary's office or a senior executive's office. For that reason, such lines are frequently exempted from the access verification so that any person can call from them at any time and the problem of unauthorized use persists.

An additional known method is to detect unauthorized use after the fact by analyzing the call durations, the direction, and the subscriber or the number called. For this purpose, the private branch exchange logs the calls made, the call destinations, call duration, and the associated PBX line. A similar verification takes place in the network management system of a public switched telephone network. For example, all calls lasting longer than a predetermined duration are checked for the call destination later or during the connection. An unauthorized use can be detected if the call destination cannot be assigned to a predetermined group of telephone numbers, which, for example, are assigned to the company's customers. Individual PBX lines such as those of senior executives can be exempted from checking for unauthorized use in this case also.

However, even with this type of checking for unauthorized use, only line-specific determination of an unauthorized use is possible. Those cases in which the same person improperly uses different terminals without authorization cannot be detected. Moreover, the unauthorized use can

only be detected after the fact; an unauthorized call cannot be prevented.

U.S. Patent 5,623,539 relates to a device and a method for monitoring a telephone connection for unauthorized use. For this purpose, voice samples of all of the persons who are authorized to use the telephone connection are stored. During a conversation conducted over the telephone connection, the transmitted voice data is tapped and broken down via suitable means into individual voice samples, each of the thus-obtained voice samples corresponding to the voice of one of the conversation participants. These voice samples taken from the telephone conversation are compared to the stored voice samples. The telephone connection is only accepted as authorized when a sufficient match between at least one of the stored voice samples and at least one of the voice samples obtained from the telephone conversation is determined.

U.S. Patent 5,093,855 relates to a method and a device for speaker recognition in a telephone switching exchange, where tapped speech samples are supplied via the telephone line to the exchange, where they are compared to previously stored speech samples. If the speaker is recognized, a first signal is emitted, otherwise, a second signal is emitted.

The publication "Speaker Identity Verification over Telephone Lines: Where we are and where we are going" by T.C. Feustel and G.A. Velius, International Carenaham Conference, Zurich 1989, addresses voice recognition and the security, e.g., against unauthorized telephone use, that it can provide. In this context, the possibility to increase security by combining voice recognition and the use of passwords or PINs is also mentioned.

Summary of the Invention

The present invention provides a method for verifying access authorization for voice telephony that does not hamper the normal use of telephones and permits direct detection of attempts at unauthorized use and prevents them if necessary. In particular, the method of the present invention provides a method for verifying access authorization for voice telephone in a fixed network or mobile telephone line by voice recognition.

According to an embodiment of the present invention, voice signals of a subscriber placing a call are recorded before or after the communication connection to the subscriber being called is set up. For example, the subscriber can be automatically prompted to acoustically provide a password after dialing the outside number, but before the connection is established. Alternatively or in addition to this embodiment, the voice signals can be recorded during the course of the call, the voice signals of the subscriber placing the call being relayed concurrently to the subscriber called so that the communication is not disturbed. In both cases, the voice signal of the subscriber placing the call is analyzed by voice recognition algorithms and compared with a reference data record or several reference data records for purposes of assignment. The reference data record(s) is/are assigned to the fixed network line or mobile telephone line in an unambiguous manner; in particular, they define the group of persons having authorized access. According to the present invention, the communication connection can be automatically disconnected or not established and/or an alarm can be triggered, if the recorded voice sample cannot be assigned to any reference data record. Otherwise, the communication connection can be maintained or established

in the customary manner.

In a further embodiment, the voice recognition can take place after the start of the communication connection online, i.e., directly during the communication connection. As with line tapping by police or intelligence services, the voice signals of the subscriber placing the call are tapped from the data line and supplied to a voice recognition unit, which analyzes them online. The voice data is transmitted concurrently to the person called. If the voice recognition unit is able to make an assignment to a reference data record, the analysis of the voice signal is terminated, and the data processing capacity of the voice recognition unit is available for identifying additional callers.

As an alternative to voice recognition during the connection, the speaker can be assigned to a billing account before the connection is established as part of an authentication procedure that the speaker must undergo. In this case, the telephone user is requested to provide a voice sample, and the connection is only established once the voice sample has been identified and the speaker is identified as authorized.

In addition to online voice recognition, the voice signal of the subscriber placing the call can also be recorded and stored in intermediate memory as a voice sample. The stored voice sample is then analyzed during or after the communication connection.

In embodiments of the present invention, it is not necessary to perform the cumbersome action of entering a password manually before the communication connection is established, but rather access is established and/or maintained by voice control. When access authorization is verified after the connection has been established, the

process takes place concurrently with the normal flow of the call; the participants do not notice the access verification, but rather they are able to talk over the telephone in the normal manner, thus saving time. The same voice signals that are transmitted to the person called are analyzed for voice recognition and subscriber identification. This does not interfere with the transmission of voice signals between the conversation participants. Thus, in principle, any connection can be monitored for unauthorized use without interfering with the normal flow of telephone conversation by additionally entering access codes.

Several possibilities for voice recognition are known and can be used to implement the present invention. There are voice recognition algorithms for recognizing semantic content of speech that compare an actual voice sample with an already stored voice sample corresponding to a specific spoken word. In this context, the stored voice sample corresponds, for example, to a spoken word whose text representation is also stored. By determining a correspondence between the actual and the stored voice sample, it is possible to assign a textual representation, e.g., in the form of an ASCII representation, to the actual voice input, thus in principle making it possible to recognize the content of a voice message. Such voice recognition units are used, for example, for the voice control of computers and the like.

Or, the future user inputs the stored voice sample during a training phase. Thus, only the actual voice input of this user may be reliably recognized by the voice recognition, since even voice samples of different users that have the same semantic content vary due to individual speech patterns.

This technique can also be used in a refinement of the present invention to verify access authorization for a telephone line. In this connection, the reference data records are reference voice samples corresponding to specific words spoken by one person, e.g., typical greetings, the first or last name of a person having authorized access or other expressions which frequently occur in a telephone conversation. These voice samples are recorded in a training phase and stored in digital form in a memory as a reference data record. In order to implement the method, the voice recognition algorithms analyze the recorded voice data for the occurrence of fragments, i.e., individual words or expressions that match the reference voice sample within a specified tolerance range. In this connection, it is not the semantic content of the reference or of the actual voice signal that is of significance, but rather the individual speech pattern of the authorized and the calling persons which is expressed in a specific characteristic pattern of the reference voice sample.

Another embodiment of the present invention also provides for the analysis of the input voice signals for speech patterns that are characteristic of the user regardless of their semantic content. The specific intonation, voice register, dialect, and the like, which cause the voice of a person to appear nearly unique to the human ear, are manifested in characteristic features of a voice sample taken from this person, e.g., a specific frequency distribution, which can be used to identify this person by electronic means. Therefore, according to the present invention, reference speech patterns, e.g., frequency patterns or amplitude patterns, which are characteristic of one person, are stored as reference data records. For example, they can be obtained by statistical analysis of a voice sample using a corresponding voice recognition algorithm. To identify the actual voice sample recorded

during a call, the voice recognition algorithms then create a corresponding speech pattern by statistically analyzing the sample. In this connection, statistical analysis primarily refers to a frequency analysis in which the tone and voice register of the speaker can be identified; dynamic analysis refers to the dynamics of the voice signal, i.e., the amplitude characteristic and, accordingly, a specific intonation. Both methods are suitable for identifying a speaker. This speech pattern is then compared with the reference speech patterns. It is determined whether the characteristic features of both patterns agree. In creating the reference speech pattern from a reference voice sample, the same voice recognition algorithm is used as that which with the actual voice sample is analyzed.

In this embodiment of the present invention, the analysis of the individual speech patterns can make a significantly more accurate identification of the speaking person possible than the search for specific words which, although individually characterized, may not always be reliably detectable due to the shortness of the words. The first variant is particularly suited for access verification by entering a specific spoken password, while the second variant is particularly suited for covertly verifying the access authorization during an ongoing call.

In a further embodiment, the reference data records correspond to the group of authorized persons, e.g., all the employees of a company who must make telephone calls as part of their work activity. The reference data records are stored, for example, in a table of authorized names. In this context, one person can be authorized only for selected telephone numbers or types of connections, or authorization can change as a function of the time of day.

The method according to the present invention can further prevent the use of terminals for the placement of toll calls by persons not belonging to this authorized group, while any authorized person can place calls from any PBX line of the company.

In another embodiment of the present invention, the access authorization can further differentiated according to PBX lines. The reference data record or reference data records are unambiguously assigned to a PBX line of a private branch exchange. The reference data record or reference data records, in turn, define the group of authorized persons, in this case for a single PBX line. This makes it possible to prevent persons authorized per se from placing telephone calls from other terminals. This is useful in the event that individual lines are cleared for interoffice calls but not for long distance calls, while this limitation does not exist for other PBX lines.

In the event of an access verification during the connection, the voice signals can be tapped during a predetermined time interval, e.g., 30 to 60 seconds, the recording starting in particular immediately after the connection is established. The voice sample is already analyzed during the tapping or at the end of the time interval.

For reasons of data security and privacy, the recorded and possibly buffered voice sample is erased after the voice recognition is completed, if it was possible to assign the sample to a reference data record. However, in the case of unauthorized use, i.e., no automatic assignment can be made to a reference data record and, accordingly, to an authorized person, the voice data preferably remains stored. It can then be used to identify the speaker.

In order to keep the expense for verifying access authorization as low as possible, the method can be implemented only at certain times of the day and/or week and/or only via specific call destinations, e.g., only for long-distance connections. The fixed network or mobile telephone line in question, or individual PBX lines of a fixed network line are then completely blocked or completely cleared for connections outside of these time periods or for other call destinations.

Moreover, it is provided that the access verification by voice recognition is not implemented if, before a connection is established, the user enters a key combination, e.g., a PIN code or an acoustic signal, e.g., a sequence of MFC signals, and has his authorization verified via this access code.

A further embodiment of the present invention provides that the number of unauthorized access attempts is recorded and the line is blocked if more than a predetermined number of such attempts is detected within a predetermined time interval, e.g., one day or one hour. In addition, an alarm can first be triggered via the network management system, and an operator can be switched in.

A further embodiment of the present invention can involve a communication network having a plurality of fixed network lines or mobile telephone lines, as well as technical means for establishing a communication connection between two or more lines of the same or of a different communication network, including:

a) means that are capable of accessing a data line via which voice signals are at least partially

transmitted from the calling line to the called line, and that are capable of recording a voice signal transmitted by the calling line;

b) at least one memory in which reference data records are stored which are assigned to a group of persons having access authorization; and

c) at least one control unit having a voice recognition unit which is capable of accessing the memory for the reference data records, analyzing the tapped voice signal via voice recognition algorithms, and determining the access authorization of the subscriber placing the call by comparison with the reference data records, the control unit initiating the production of a signal to disconnect the connection if the voice signal cannot be assigned to any of the reference data records,

so that voice samples are recorded at regular time intervals during the entire communication connection, and the speaker's authorization is checked at regular time intervals.

In this context, a communication network can be understood to be the totality of all lines including the exchanges or conversion stations and possibly data lines and other intelligent switching and transmission devices. The elements involved in the present invention can, however, be arranged in only a small part of the network, e.g., in a private branch exchange. The communication network according to the present invention advantageously makes it possible to verify the access authorization of users of individual lines and accordingly to implement the method according to the invention.

In order to be able to utilize the voice signals in a detected case of abuse, to identify the unauthorized

caller or for offline voice analysis, the communication network may have at least one memory in which the recorded voice signals are stored in intermediate memory as voice samples.

According to the present invention, the verification of access authorization within the communication network can take place at various points within the network. If the access authorization of users of a private branch exchange is to be verified, the control unit and the reference data memory or possibly the voice sample memory can be arranged within the private branch exchange. The control unit can be, for example, part of a data processing system that logs the connections made by the individual PBX lines, blocks individual PBX lines on a time-dependent basis or for specific call destinations, and possibly requests a PIN code.

Alternatively, the control unit and the corresponding memory locations can be located outside the customer area in an exchange in the actual telephone network. In this case, the reference data of the lines assigned to the exchange can be stored in the reference data memory. Preferably, the reference data is stored in a line-specific manner, so that an authorized group of persons is defined for each line and is checked by the exchange. If the control unit is unable to assign the voice sample to any of the reference data records, it causes the exchange to generate a signal disconnecting the connection. In this manner, a common control unit can be used to centrally verify the access authorization of users of a plurality of lines in the exchange without requiring a modification of the lines on the customer side.

Access verification can be further centralized by assigning the control unit and the corresponding memory to an SCP (Service Control Point) of an intelligent network and by the control unit causing the SCP to generate a signal interrupting the connection if the voice sample cannot be assigned to any of the reference data records. The so-called intelligent network is an open communications network, which is built on the traditional telephone network and makes various telephone services having new features possible, for example, toll-free calling using specific numbers or reaching various offices of a corporation using a dial number that is identical over a larger region. The central computer containing the required switching information is known as the SCP. The transition from a telephone network of one network provider to that of a different network provider is also accomplished using structures similar to an IN.

In addition, the method according to the present invention can also be used to check the authorization of a mobile terminal user. For this purpose, a mobile terminal for telecommunications is proposed, including:

a) means that are capable of accessing a data line, via which voice signals are transmitted in electronic form, and of recording an entered signal and a voice signal;

b) at least one memory in which at least one or more reference data records are stored which are assigned to a group of persons having access authorization; and

c) at least one control unit having a voice recognition unit which is capable of accessing the memory for the reference data records, analyzing the tapped voice signal via voice recognition algorithms, and of determining the access authorization of the

subscriber placing the call by comparison with the reference data records, the control unit initiating the production of a signal to disconnect the connection or causing the terminal to shut off if the voice signal cannot be assigned to any of the reference data records,

so that voice samples are recorded at regular time intervals during the entire communication connection, and the speaker's authorization is checked at regular time intervals.

The reference data record(s) can be stored on the chip of a mobile telephone card. The owner of the mobile telephone can provide the voice sample necessary for this purpose when purchasing the mobile telephone card. Therefore, a lost mobile telephone is, in principle, operable, but the mobile telephone card is only operable as a function of the correct speech pattern. This can prevent calls from continuing to be made on a lost mobile telephone at the owner's expense.

Brief Description of the Drawings

Figure 1 shows a schematic of the sequence of operations of an embodiment of the present invention;

Figure 2 shows a flowchart of another embodiment of the present invention;

Figure 3a shows a communication network used with an embodiment of the present invention;

Figure 3b shows a communication network used with an embodiment of the present invention;

Figure 4a shows a communication network used with an embodiment of the present invention;

Figure 4b shows a communication network used with an

embodiment of the present invention;

Figure 4c shows a communication network used with an embodiment of the present invention; and

Figure 5 show a communication network used with an embodiment of the present invention.

Detailed Description

Figure 1 schematically shows a sequence of operations of an embodiment of the method of the present invention. At the start of the method, subscriber A calls a destination number. The connection is established as soon as subscriber B answers. Typically, both subscribers begin to speak. The voice signals of subscriber A are automatically tapped and analyzed, the analysis lasting a predetermined time span, approximately 30 seconds to one minute. A interoffice trunk, via which the voice signals between both users are transmitted, is accessed without interfering with the transmitted signal, so that the access verification does not affect the conversation.

The voice signal of subscriber A is analyzed, i.e., compressed by voice recognition algorithms, the thus-produced speech pattern being compared with reference data records stored in a table of authorized names. If the actual voice signal can be assigned to one of the reference data records, then the subscriber is considered to be authorized and entitled to call. In this context, the table of authorized persons can refer specifically to the line as a whole or to a PBX line and/or it may be time-dependent.

If subscriber A is approved, then the connection is maintained until the end of the call. In the simplest case, no additional check is made. To further increase

security against abuse, the process is repeated at regular time intervals, i.e., the voice signal of subscriber A is analyzed again.

If the subscriber is identified as unauthorized, because his voice signal cannot be assigned to an entry in the table of authorized persons, the connection is interrupted in the simplest case by generating a interrupting signal or by briefly deactivating the terminal. A new connection can be established immediately after the connection is terminated.

To counteract persistent attempts at unauthorized use, it is also possible to record the number of attempts at unauthorized use within a specific time interval and to set a critical value for the maximum number to be tolerated. If the number of attempts at unauthorized use exceeds this value, a total block of the line is automatically initiated. The line can then only be enabled again after a specific waiting period or by the entering an enabling code. In addition, as in the case of a normal termination due to unauthorized use, an alarm signal can be produced at the telephone itself or at a PBX operator desk.

Figure 2 shows an additional flowchart of the method according to the present invention. Before the method is initiated, all users of the telephone line to be protected against abuse enter voice samples into the system. The voice recognition unit or a speech pattern recognition system extracts the subscribers' speech patterns and stores them, compressed by a voice recognition algorithm, in memory as reference data. The reference speech patterns are, thus, available for online recognition at the facilities of the network provider, in

a private branch exchange, or on the calling card of a mobile telephone.

The process begins once a caller initiates a call from a telephone, the telephone connection is established by the network provider, and the telephone conversation is started. At the same time as the telephone call, the speech pattern recognition is initiated to determine the speech pattern of the caller. This speech pattern determined for the caller from the telephone call is compared with the reference stored for this line or on the calling card of a mobile telephone.

If a speech pattern is recognized, i.e., the actual voice signal matches a reference, the speech pattern recognition for this connection is discontinued, and the computer capacity can be used to analyze other calls.

If no speech pattern is recognized, the call is interrupted to protect the customer from financial loss. When a mobile telephone is used with a calling card, the call is always terminated. If necessary, the customer can be provided with a log of the attempt at unauthorized use in order to identify the person using the telephone without authorization.

Figures 3 through 5 show three possibilities for implementing the method according to the present invention in a communications network.

For this purpose, Figure 3A shows a private branch exchange (PBX), which is connected to a public switched telephone network. The private branch exchange (PBX) has a plurality of extension stations, of which three are shown here. The access authorization of the users of the

individual extension stations is to be monitored according to the present invention. For this purpose, an IP (intelligent peripheral) is assigned to the private branch exchange (PBX), the IP being capable of accessing the telephone line via which signals are transmitted from one extension station to an additional line outside the private branch exchange, and of recording and storing the signals entered by the extension station user. In addition, the IP has a voice recognition unit that is capable of analyzing the recorded voice signal and comparing it with previously stored reference data records. In addition, the IP is also capable of accessing the reference data record memory. In this case, either specific reference data records are assigned to each extension station, the reference data records being assigned to the users of this extension station, or the table of authorized persons contains all potential users of the entire private branch exchange irrespective of the actual PBX line.

If the IP cannot match the actual voice sample to any of the reference data records, it applies a suitable control signal to induce the private branch exchange (PBX) to generate a signal interrupting the connection. As a result, the connection of a PBX line to a user in the public switched telephone network via the private branch exchange is interrupted.

Figure 3B shows an example for the implementation of person-specific assignment of charges by voice recognition in a private branch exchange.

In the private branch exchange, in the case of procedural authentication, i.e., voice recognition before a connection is established, all calls originating from the

terminals connected to PBX lines (ports 22 to 28) are redirected to one port (port 21 in the illustrated example). This redirection is performed by the control unit of the private branch exchange. The relevant programs are stored, for example, in a memory module, an EEPROM in this case. A digital signal processor (DSP) having suitable voice recognition software and, optionally, voice recognition hardware is connected to port 21. If the identification is positive, it relays the signal to the private branch exchange via the customary control functions, i.e., either via the line, a V.24 interface, or another management interface. The thus-verified calls are switched from the private branch exchange (PBX) to the interexchange trunk and form an outgoing call. The billing information for person-specific cost assignment is fed directly into the billing system.

In the case of online recognition of the speaker, the call is already set up; however, as in the case of "bugging" a call, the call information is serially routed through the DSP. The DSP analyzes the speech without interfering with the transmission and relays corresponding information to the private branch exchange or the billing system.

Figure 4A shows an arrangement of control unit IP corresponding to the arrangement of Figure 3A in an exchange. A connection from the subscriber line to an additional line in the public switched telephone network is established via this exchange. Physically and organizationally, the exchange is assigned to the subscriber line; however, it is not necessarily located in its immediate vicinity. Aside from the different physical arrangement of the IP, the access verification

is performed here in the same manner as described above. The difference is that no intelligent devices for voice recognition and for speech storage need to be provided on the subscriber side, since these are centrally integrated in the exchange.

Figure 4B shows an example for the implementation of access verification by voice recognition in an exchange of a telephone network.

Voice recognition system IP can be implemented in a computer, for example in the form of a plug-in module in the exchange. Calls for which the speaker is to be identified are routed from the exchange through the IP.

Voice recognition is implemented either in dialog form, i.e., an authentication procedure is executed as described above in Figure 3B, or else the voice is recognized online. In the latter case, the speech pattern is checked during the conversation in progress and characteristics of the speech of speaking user A are compared with the stored patterns. In this case, the call is tapped, so to speak, by the IP without interfering with it.

One possible structure for the authentication procedure is a dial-in into the DSP of the IP. For this purpose, the telephone channel is routed to an input of the IP. At this point, subscriber A is asked by the software of an intelligent voice response system to state his name or his identifier. After that, he is asked for his password or his personal identification number PIN. The data is compared with the identifier stored in memory, and the speech pattern is compared with the stored patterns either using frequency spectra or speech dynamics. In the

dialog form, the implementation of voice recognition is very simple, since the identifier is made up of precisely defined words, which were previously entered.

After authentication in the IP, the customer is directed to a menu that requests that he enter the desired telephone numbers. These are recorded as in conventional messaging or voice response systems, converted into pulse or MFC dialing information, and sent into the network, or they are relayed to the exchange as signals in the format of signaling system No. 7 (Common Channel Number 7, CCS7). The exchange then initiates the connection to subscriber B. The use of CCS7 signals permits faster processing and more features, namely all those implemented in CCS7 and cleared for the IP.

The information concerning the speaker, i.e., the identified reference data record, is sent as control information to the exchange via the CCS7, and generates an alarm in the network management system. The network management system can also generate a corresponding alarm message regarding call data records, so that the billing system also receives appropriate information.

The speaker-identifying data records produced in this way are used for access verification; however, they can also be used for billing a call. The corresponding procedures are described in the flowcharts.

When recognizing continuous speech, the system preferably concentrates on the essential characteristics of the language. To be sure, key words such as "good morning, hello," etc. can be considered in the entry procedure; however, in principle, it is necessary to store speaker-specific characteristics, irrespective of which language

and with whom the user is speaking. For this purpose, the algorithm can use static methods such as frequency spectrum analysis, as well as dynamic speech characteristics.

Figure 4C shows an additional example of the method according to the present invention implemented in an exchange. The subscriber unit (subscriber card) of subscriber A recognizes whether the subscriber has provided voice recognition for access verification. The central processing unit CPU of the exchange initiates the appropriate routing through the switching matrix, the actual switching unit. As a result, the call is not routed directly to subscriber B or to the next exchange, but rather it is first routed through an intelligent peripheral IP having a digital signal processor (DSP). The output port of the IP is routed through the switching matrix to subscriber B or to the next exchange.

All control information and, accordingly, also the result of the voice recognition are compared in the exchange having the central processing unit CPU.

The IP can also include several voice recognition units or DSPs and, thus, analyze several lines simultaneously. The information concerning the usage of the IP and concerning the analytical results is transmitted to the CPU.

Figure 5 shows the implementation of the method according to the present invention in the service control point SCP of an intelligent network.

When implemented in the IN, the voice data is routed via an ISDN channel to voice recognition unit IP, which is

located at the site of the SCP. Control information, for example, whether the calling line is using voice recognition for monitoring abuse, results from the voice analysis, and the like are then exchanged between the SCP and the service switching point SSP, which is located at the site of the exchange.

Implementing the method according to the present invention in the centrally structured IN makes it possible to centrally implement voice-based abuse control over a large network area, i.e., a plurality of lines. This eliminates the need for expensive software and hardware equipment in the exchanges; only the IN must be adapted. This implementation is, therefore, suitable in particular for cases of low demand or in the introductory phase, i.e., it is not yet worthwhile to equip each exchange.

The present invention is suitable, in particular, for operators of communication networks to increase the security of voice telephony customers against abuse. Moreover, the present invention is particularly suitable for operators of private branch exchanges where the problem of unauthorized access is encountered on a regular basis.

Abstract

A method for verifying access authorization for voice telephony in a fixed network line or mobile telephone line, as well as a communications network having such access authorization verification are described. The access authorization is verified by analysis of a voice signal which was entered by the subscriber placing the call, before or during a call in progress. In one variant, the voice signal is entered as a password before the connection is established; in another variant, voice signals are analyzed for voice recognition and subscriber identification, the same voice signals also being transmitted to the person being called, making concealed access verification possible which does not hamper the normal flow of conversation.

09/786819
JC02 Rec'd PCT/PTO 0 9 MAR 2001

[
]

METHOD FOR VERIFYING ACCESS AUTHORIZATION FOR VOICE TELEPHONY IN A FIXED NETWORK LINE OR MOBILE TELEPHONE LINE AS WELL AS A COMMUNICATIONS NETWORK

[Technical]

Field of the Invention

The present invention relates to a method for verifying access authorization for voice telephony in a fixed network line or mobile telephone line as well as a communications network [with]having such access authorization verification.

Background [Information]of the Invention

[With]In the case of private branch exchanges (PBXs) for telecommunications having a large number of extension stations used by different persons, but also [with]in the case of mobile terminals[, in other words,] such as cell phones, there exists the problem of abuse by unauthorized third parties or by unauthorized employees of a company. For example, personal conversations are frequently [carried on from]held via PBX lines of large corporations at the employer's expense. Moreover, when telephone calls are made from a stolen or lost mobile telephone[or one that has otherwise gone astray], the account of the lawful owner is always charged without the owner being able to directly prevent this.

To prevent unauthorized use in private branch exchanges, methods are known in which the user of a terminal must enter an access code to be able to make an interoffice call and/or to dial specific outside numbers. In these methods, the subscriber[ ]_enters a personal access code

EL302703433

(PIN) via the keypad of the terminal, the access code being evaluated by the private branch exchange and compared with a table of authorized names. This method also makes [allocation of]it possible to allocate the incurred charges to specific individuals[possible]. Once the subscriber's authorization has been established in this manner, the corresponding PBX line is enabled to establish an interoffice or long[-]-distance connection.

However, due to the additional time required, this method of entering a code before each call is very cumbersome and is not [practicable]practical for PBX lines from which many calls are made regularly, e.g., a secretary's office or a senior executive's office[, due to the additional time required]. For that reason, such lines are frequently exempted from the access verification[,] so that any person can call from them at any time and the problem of unauthorized use [continues to exist]persists.

An additional known method is to detect unauthorized use after the fact by analyzing the call durations, the direction, and the subscriber[called] or the number called. For this purpose, the private branch exchange logs the calls made, the call destinations, call duration, and the associated PBX line. A similar verification takes place in the network management system of a public switched telephone network. For example, all calls lasting longer than a predetermined duration are checked for the call destination later or during the connection. An unauthorized use can be detected if the call destination cannot be assigned to a predetermined group of telephone numbers, which, for example, are assigned to the company's customers. Individual PBX lines such as those of senior executives can be exempted from checking for unauthorized use in this case also.

However, even with this type of checking for unauthorized use, only line[-]-specific determination of an unauthorized use is possible. Those cases in which the same person improperly uses different terminals without authorization cannot be detected. Moreover, the unauthorized use can only be detected after the fact[, while]; an unauthorized call cannot be prevented.

[Technical Object

The object of the]U.S. Patent 5,623,539 relates to a device and a method for monitoring a telephone connection for unauthorized use. For this purpose, voice samples of all of the persons who are authorized to use the telephone connection are stored. During a conversation conducted over the telephone connection, the transmitted voice data is tapped and broken down via suitable means into individual voice samples, each of the thus-obtained voice samples corresponding to the voice of one of the conversation participants. These voice samples taken from the telephone conversation are compared to the stored voice samples. The telephone connection is only accepted as authorized when a sufficient match between at least one of the stored voice samples and at least one of the voice samples obtained from the telephone conversation is determined.

U.S. Patent 5,093,855 relates to a method and a device for speaker recognition in a telephone switching exchange, where tapped speech samples are supplied via the telephone line to the exchange, where they are compared to previously stored speech samples. If the speaker is recognized, a first signal is emitted, otherwise, a second signal is emitted.

The publication "Speaker Identity Verification over Telephone Lines: Where we are and where we are going" by T.C. Feustel and G.A. Velius, International Carenaham Conference, Zurich 1989, addresses voice recognition and the security, e.g., against unauthorized telephone use, that it can provide. In this context, the possibility to increase security by combining voice recognition and the use of passwords or PINs is also mentioned.

Summary of the Invention

The present invention [is therefore to]provides a method for verifying access authorization for voice telephony [which]that does not hamper the normal use of telephones and permits direct detection of attempts at unauthorized use and prevents them if necessary.[

Summary] In particular, the method of the [I]present invention[

The objective is achieved by] provides a method for verifying access authorization for voice telephon[y]e in a fixed network or mobile telephone line by voice recognition[according to Claim 1. Advantageous further developments of the invention are the object of the dependent claims].

According to an embodiment of the present invention, voice signals of [the]a subscriber placing [the]a call are recorded before or after the communication connection to the subscriber being called [user]is set up. For example, the subscriber can be automatically [requested]prompted to acoustically provide a password

after dialing the outside number, but before the connection is [set up]established. Alternatively or in addition to this embodiment, the voice signals [are]can be recorded during the course of the call, the voice signals of the subscriber placing the call[er] being relayed concurrently to the subscriber called so that the communication is not disturbed. In both cases, the voice signal of the subscriber placing the call is analyzed by voice recognition algorithms and compared with a reference data record or several reference data records for purposes of assignment. The reference data record(s) is/are assigned to the fixed network line or mobile telephone line in an unambiguous manner; in particular, they define the group of persons having authorized access. According to the present invention, the communication connection [is]can be automatically [interrupted]disconnected or[is] not established and/or an alarm [is]can be triggered, if the recorded voice sample cannot be assigned to any reference data record. Otherwise, the communication connection [is]can be maintained or established in the customary manner.

[Preferably]In a further embodiment, the voice recognition can take[s] place after the start of the communication connection online, i.e., directly during the communication connection. As with line tapping by police or intelligence services, the voice signals of the subscriber placing the call are tapped from the data line and supplied to a voice recognition unit, which analyzes them online. The voice data [are]is transmitted concurrently to the person called. If the voice recognition unit is able to make an assignment to a reference data record, the analysis of the voice signal is terminated, and the data processing capacity of the voice recognition unit is available for identifying

additional callers.

As an alternative to voice recognition during the connection, the speaker can be assigned to a billing account before the connection is established as part of an authentication procedure [which]that the speaker must undergo. In this case, the telephone user is requested to provide a voice sample, and the connection is only established once the voice sample has been identified and the speaker is identified as authorized.

In addition to online voice recognition, the voice signal of the subscriber placing the call can also be recorded and stored in intermediate memory as a voice sample. The stored voice sample is then analyzed [still]during or after the communication connection.

[The method according to]In embodiments of the present invention[has the great advantage that before the communication connection is made], it is not necessary to perform the cumbersome action of entering a password manually before the communication connection is established, but rather access is established [or]and/or maintained by voice control. When access authorization is verified after the connection has been established, the process takes place concurrently with the normal flow of the call[,]; the participants [noticing nothing of]do not notice the access verification, but rather they are able to talk over the telephone in the normal manner, thus saving time. The same voice signals that are transmitted to the person called are analyzed for voice recognition and subscriber identification. This does not interfere with the transmission of voice signals between the [call]conversation participants. Thus, in principle, any connection can be monitored for unauthorized use without

interfering with the normal flow of telephone conversation by [the]additional[entry of]ly entering access codes.

Several possibilities for voice recognition are known and can be used to implement the present invention. There are voice recognition algorithms for [the recognition of]recognizing semantic content [which]of speech that compare an actual voice sample with an already stored voice sample [which corresponds]corresponding to a specific spoken word. [T]In this context, the stored voice sample corresponds, for example, to a spoken word whose text representation is also stored. By determining a correspondence between the actual and the stored voice sample, it is possible to assign a textual representation, e.g., in the form of an ASCII representation, to the actual voice input, thus in principle making it possible to recognize the content of a voice message. Such voice recognition units are used, for example, for the voice control of computers and the like.

[Typically]Or, the future user inputs the stored voice sample during a training phase. [The typical result is that, even in this case]Thus, only the actual voice input of [the]this user [can]may be reliably recognized[reliably] by the voice recognition, since even voice samples of different users that have the same semantic content vary due to individual speech patterns.

This [principle]technique can also be used in a refinement of the present invention to verify access authorization for a telephone line. In this connection, the reference data records are reference voice samples corresponding to specific words spoken by one person,

e.g., typical greetings, the first or last name of a person [with]having authorized access or other expressions which frequently occur in a telephone conversation. These voice samples are recorded in a training phase and stored in digital form in a memory as a reference data record. In order to implement the method, the voice recognition algorithms analyze the recorded voice data for the occurrence of fragments, i.e., individual words or expressions that match the reference voice sample within a specified tolerance range. In this connection, it is not the semantic content of the reference or of the actual voice signal that is of significance, but rather the individual speech pattern of the authorized and the calling persons which is expressed in a specific characteristic pattern of the reference voice sample.

[For this reason, a]Another[preferred] embodiment [does not provide for the use of an actual word recognition system like the one described previously, but rather]of the present invention also provides for the analysis of the input voice signals for speech patterns that are characteristic of the user regardless of their semantic content. The specific intonation, voice register, dialect, and the like, which cause the voice of a person to appear nearly unique to the human ear, are manifested in characteristic features of a voice sample taken from this person, e.g., a specific frequency distribution, which can be used to identify this person by electronic means. Therefore, according to the present invention, reference speech patterns, e.g., frequency patterns or amplitude patterns, which are characteristic of one person, are stored as reference data records. For example, they [are]can be obtained by statistical analysis of a voice sample using a corresponding voice

recognition algorithm. To identify the actual voice sample recorded during a call, the voice recognition algorithms then create a corresponding speech pattern by statistical[analysis of]ly analyzing the sample. In this connection, statistical[] analysis primarily refers to a frequency analysis in which the tone and voice register of the speaker can be identified; dynamic analysis refers to the dynamics of the voice signal, i.e., the amplitude characteristic and, accordingly, a specific intonation. Both methods are suitable for identifying a speaker. This speech pattern is then compared with the reference speech patterns. It is determined whether the characteristic features of both patterns agree. In creating the reference speech pattern from a reference voice sample, [it is important that]the same voice recognition algorithm [be]is used [with]as that which with the actual voice sample is analyzed.

[The advantage]In this embodiment of [this variant is that]the present invention, the analysis of the individual speech patterns can make[s an essentially] a significantly more accurate identification of the speaking person possible than the search for specific words which, although individually characterized, may not always be reliably detectable due to the shortness of the words. The first variant is [suited in particular]particularly suited for access verification by entering a specific spoken password, while the second variant is [suited in particular]particularly suited for covertly verifying the access authorization during an ongoing call.

[T]In a further embodiment, the reference data records correspond to the group of authorized persons, e.g., all the employees of a company who must make telephone calls

as part of their work activity. The reference data records are stored, for example, in a table of authorized names. [O]In this context, one [person's authorization may apply]person can be authorized only [to]for selected telephone numbers or types of connections, or authorization can change as a function of the time of day.

The method according to the present invention can [advantageously]further prevent the use of terminals for the placement of toll calls by persons not belonging to this authorized group, while any authorized person can place calls from any PBX line of the company.

In [an additional advantageous refinement]another embodiment of the present invention, the access authorization [is]can further differentiated according to PBX lines. The reference data record or [the]reference data records are [assigned]unambiguously assigned to a PBX line of a private branch exchange. The reference data record or reference data records, in turn, define the group of authorized persons, in this case for a single PBX line. This makes it possible to prevent persons authorized per se from placing telephone calls from other terminals. This is [important]useful in the event that individual lines are cleared for interoffice calls but not for long distance calls, while this limitation does not exist for other PBX lines.

In the event of an access verification during the connection, the voice signals [are]can be tapped during a predetermined time interval, e.g., 30 to 60 seconds, the recording starting in particular immediately after the

connection is established. The voice sample is already analyzed[already] during the tapping or at the end of the time interval.

[For long-term monitoring of the access authorization of the subscriber placing the call, it is further provided that the voice signals are analyzed at regular intervals during the connection and used to check the speaker's authorization at regular time intervals. In this manner, it is also possible to detect a change of speakers and interrupt the connection, if appropriate.

]For reasons of data security and privacy, the recorded and possibly buffered voice sample is erased after the voice recognition is completed, if it was possible to assign the sample to a reference data record. However, in the case of unauthorized use, i.e., no automatic assignment can be made to a reference data record and, accordingly, to an authorized person, the voice data [is]preferably [kept in storage]remains stored. It can then be used to identify the speaker.

In order to keep the expense for verifying access authorization as low as possible, [it is advantageous if]the method [is]can be implemented only at certain times of the day and/or week and/or only via specific call destinations, e.g., only for long[-]-distance connections. The fixed network or mobile telephone line in question, or individual PBX lines of a fixed network line are then [totally]completely blocked or [totally]completely cleared for connections outside of these time periods or for other call destinations.

Moreover, it is provided that the access verification by voice recognition is not implemented if, before a connection is established, the user enters a key combination, e.g., a PIN code or an acoustic signal, e.g., a sequence of MFC signals, and has his authorization verified via this access code.

A[n additional advantageous refinement] <u>further embodiment</u> of the present invention provides that the number of unauthorized access attempts is recorded and the line is blocked if more than a predetermined number of such attempts is detected within a predetermined time interval, e.g., one day or one hour. In addition, an alarm can first be triggered via the network management system<u>,</u> and an operator can be switched in.

[The object is furthermore attained by]<u>A further embodiment of the present invention can involve</u> a communication network [which may be a]<u>having a plurality of</u> fixed network <u>lines</u> or[a] mobile [telephony network. According to the present invention, the network has means which]<u>telephone lines, as well as technical means for establishing a communication connection between two or more lines of the same or of a different communication network, including:</u>

<u>a)</u> <u>means that</u> are capable of accessing a data line via which voice signals are at least partially transmitted from the calling line to the called line<u>,</u> and<u> that</u> are capable of recording a voice signal transmitted by the calling line[. Moreover,]<u>;</u>

<u>b)</u> at least one memory[is present] in which reference data records are stored which are assigned to a

group of persons having access authorization[. Moreover,]; and

c) at least one control unit having a voice recognition unit [is present,]which is capable of accessing the memory for the [voice samples and the]reference data records[and], analyzing the [stored]tapped voice [sample using]signal via voice recognition algorithms, and determining the access authorization of the subscriber placing the call by [comparing them]comparison with the reference data records[. In doing so], the control unit [causes a signal which clears the connection or an alarm signal to be generated]initiating the production of a signal to disconnect the connection if the voice signal cannot be assigned to any [one]of the reference data records,

so that voice samples are recorded at regular time intervals during the entire communication connection, and the speaker's authorization is checked at regular time intervals.

[A]In this context, a communication network [is]can be understood to be the totality of all lines [with]including the exchanges or conversion stations and possibly data lines and other intelligent switching and transmission devices. The elements involved in the present invention can, however, be arranged in only a small part of the network, e.g., in a private branch exchange. The communication network according to the present invention advantageously makes it possible to verify the access authorization of users of individual lines and accordingly to implement the method [of]according to the invention.

In order to be able to utilize the voice signals in a detected case of abuse, to identify the unauthorized caller or for offline voice analysis, the communication network [preferably]may ha[s]ve at least one memory in which the recorded voice signals are stored in intermediate memory as voice samples.

According to the present invention, the verification of access authorization within the communication network can take place at various points within the network. If the access authorization of users of a private branch exchange is to be verified, [then]the control unit and the reference data memory or possibly the voice sample memory [are preferably]can be arranged within the private branch exchange. The control unit [is]can be, for example,[a] part of a data processing system [which]that logs the connections made [from]by the individual PBX lines, blocks individual PBX lines on a time[-]-dependent basis or for specific call destinations, and possibly [queries for]requests a PIN code.[ ]

Alternatively, the control unit and the corresponding memory locations [may]can be located outside the customer area in an exchange in the actual telephone network. In this case, the reference data of the lines assigned to the exchange [are]can be stored in the reference data memory. Preferably, the reference data is stored in a[re line-specific] line-specific manner, so that an authorized group of persons is defined for each line and is checked by the exchange. If the control unit is unable to assign the voice sample to any of the reference data records, it causes the exchange to generate a signal [clearing]disconnecting the connection. In this manner, a

common control unit can be used to centrally verify the access authorization of users of a [large number]plurality of lines [centrally from]in the exchange[,] without requiring a modification of the lines on the customer side.

Access verification can be further centralized[, in that] by assigning the control unit and the corresponding memory[are assigned] to an SCP (Service Control Point) of an intelligent network[,] and [in that]by the control unit [induces]causing the SCP to generate a signal [clearing]interrupting the connection[,] if the voice sample cannot be assigned to any of the reference data records. The so[-]-called intelligent network is an open communications network, which is built on the traditional telephone network[, which] and makes various telephone services [with]having new features possible, for example, toll[-]-free calling using specific numbers or reaching various offices of a corporation using a dial number [which]that is identical over a large[territory]r region. The central computer containing the required switching information is known as the SCP. [Also, t]The transition from a telephone network of one network provider to that of a different network provider is also accomplished using structures similar to an IN.

In addition, the method according to the present invention can also be used to check the authorization of a mobile terminal user. For this purpose, a mobile terminal [having the following features is proposed]for[the] telecommunications is proposed, including:

[

]a)[Means are provided which] means that are capable

of accessing a data line, via which voice signals are transmitted in electronic form, and of recording an entered signal and a voice signal[.]<u>;</u>

b) [At] <u>at</u> least one memory[is provided] in which at least one [reference data record]or [several]<u>more</u> reference data records are stored[,] which are assigned to a group of persons having access authorization[.]<u>; and</u>

c) [At] <u>at</u> least one control unit having a voice recognition unit[is provided] which is capable of accessing the memory for the reference data records[and]<u>,</u> analyzing the tapped voice signal via voice recognition algorithms, and of determining the access authorization of the subscriber placing the call by comparison with the reference data records, the control unit initiating the production of a signal to [clear]<u>disconnect</u> the connection or [disconnect]<u>causing</u> the terminal <u>to shut off</u> if the voice signal cannot be assigned to any of the reference data records<u>,</u>

<u>so that voice samples are recorded at regular time intervals during the entire communication connection, and the speaker's authorization is checked at regular time intervals</u>.[ ]

The reference data record(s) [is/are preferably]<u>can be</u> stored on the chip of a mobile telephone card. The owner

of the mobile telephone [preferably]can provide[d] the voice sample necessary for this purpose when purchasing the mobile telephone card. [A]Therefore, a lost mobile telephone is[thus], in principle, operable, but the mobile telephone card is only operable as a function of the correct speech pattern. This can prevent calls from [being]continuing to be made on a lost mobile telephone at the owner[']'s expense.

Brief [d]Description of the [drawing in which:

Figure 1]Drawings

Figure 1 shows a schematic of the sequence of operations of an embodiment of the present invention;

Figure 2 shows a flowchart of another embodiment of the present invention;

Figure 3a shows a communication network used with an embodiment of the present invention;

Figure 3b shows a communication network used with an embodiment of the present invention;

Figure 4a shows a communication network used with an embodiment of the present invention;

Figure 4b shows a communication network used with an embodiment of the present invention;

Figure 4c shows a communication network used with an embodiment of the present invention; and

Figure 5 show a communication network used with an embodiment of the present invention.

Detailed Description

Figure 1 schematically shows [the]a sequence of operations of an embodiment of the method [according to]of the present invention[;

Figure 2 shows an additional flowchart of the method according to the present invention;

Figures 3-5 show examples of communication networks for implementing the method according to the present invention.

The sequence of operations of the method according to the present invention is schematically shown in Figure 1.]. At the start of the method, subscriber A calls a destination number. The connection is established as soon as subscriber B answers. [B]Typically, both subscribers begin to speak[normally]. The voice signals of subscriber[s] A are automatically tapped and analyzed, the analysis lasting[for] a predetermined time span, approximately 30 seconds to one minute. [Access to an]A interoffice trunk, via which the voice signals between both users are transmitted[between both subscribers], [takes place]is accessed without [interference]interfering with the transmitted signal, so that the access verification does not affect the conversation.

The voice signal of subscriber A is analyzed, i.e., compressed by voice recognition algorithms, the thus-produced speech pattern[thus produced] being compared with reference data records stored in a table of authorized names. If the actual voice signal can be assigned to one of the reference data records, then the subscriber is considered to be authorized and entitled to call. [T]In this context, the table of authorized persons

can refer specifically to the line as a whole or to a PBX line[,] and/or it may be time[-]-dependent.

If [caller]subscriber A is approved, then the connection is maintained until the end of the call. In the simplest case, no additional check is made. [However, t]To further increase security against abuse, the process [can be]is repeated at regular time intervals, i.e., the voice signal of subscriber A is analyzed again.

If the subscriber is identified as unauthorized, because his voice signal cannot be assigned to an entry in the table of authorized persons, the connection is interrupted in the simplest case by [the generation of]generating a [clearing]interrupting signal or by briefly deactivating the terminal[for only a brief time. In principle, it is then possible to establish a new connection]. A new connection can be established immediately after the connection is [interrupted]terminated.

To counteract persistent attempts at unauthorized use, it is also possible to record the number of attempts at unauthorized use within a specific time interval and to set a critical value for the maximum number to be tolerated. If the number of attempts at unauthorized use exceeds this value, a total block of the line is [initiated]automatically initiated. The line can then only be enabled again after a specific waiting period or by the [entry of]entering an enabling code. In addition, as [with]in the case of a normal [interruption]termination due to unauthorized use, an alarm signal can be produced at the telephone itself or

at a PBX operator desk.

Figure 2 shows an additional flowchart of the method according to the present invention. Before the method is initiated, all [subscribers]users of the telephone line to be protected against abuse enter voice samples into the system. The voice recognition unit or a speech pattern recognition system extracts the subscribers[']' speech patterns and stores them,[after compressing them using] compressed by a voice recognition algorithm, [stores them]in memory as reference data. The reference speech patterns are, thus, available for online recognition at the facilities of the network provider, in a private branch exchange, or on the calling card of a mobile telephone.

The process begins once a caller initiates a call from a telephone, the telephone connection is established by the network provider, and the telephone conversation is started. [T]At the same time as the telephone call, the speech pattern recognition is initiated[simultaneously with the telephone call,] to determine the speech pattern of the caller.[

]_This speech pattern determined for the caller from the telephone call is compared with the reference stored for this line or on the calling card of a mobile telephone.

If a speech pattern is recognized, i.e., the actual voice signal matche[d]s a reference, the speech pattern recognition for this connection is discontinued[;]_ and the [respective]computer capacity can be used to analyze other calls.

If no speech pattern is recognized, the call is interrupted to protect the customer from financial loss. When a mobile telephone is used with a calling card, the call is always terminated. If necessary, the customer can be provided with a log of the attempt at unauthorized use[,] in order to identify the person using the telephone without authorization.

Figures 3 [to]through 5 show three possibilities for implementing the method according to the present invention in a communications network.

For this purpose, Figure 3A shows a private branch exchange (PBX), which is connected to a public switched telephone network. The private branch exchange (PBX) has a [large number]plurality of extension stations, of which three are shown here. The access authorization of the [subscribers]users of the individual extension stations is to be monitored according to the present[ ] invention. For this purpose, an IP (intelligent peripheral) is assigned to the private branch exchange (PBX)[. T], the IP [is]being capable of accessing the telephone line[,] via which signals are transmitted from one extension station to an additional line outside the private branch exchange[are transmitted], and of recording and storing the signals entered by the extension station [subscriber]user. In addition, the IP has a voice recognition unit [which]that is capable of analyzing the recorded voice signal and comparing it with previously stored reference data records. In addition, the IP is also capable of accessing the reference data record memory. In this case, either specific reference data records are assigned to each extension station, the

reference data records being assigned to the [subscribers]users of this extension station, or the table of authorized persons contains all potential [subscribers]users of the entire private branch exchange[,] irrespective of the actual PBX line.

If the IP cannot match the actual voice sample to any of the reference data records, it applies a suitable control signal to induce the private branch exchange (PBX) to generate a signal [clearing]interrupting the connection. As a result, the connection of a PBX line to a [subscriber]user in the public switched telephone network via the private branch exchange is interrupted.

Figure 3B shows an example for the implementation of person[-]-specific assignment of charges by voice recognition in a private branch exchange.

In the private branch exchange, in the case of procedural authentication, i.e., voice recognition before a connection is established, all calls originating from the terminals connected to PBX lines (ports 22 to 28) are redirected to one port (port 21 in the [example]illustrated example). This redirection is performed by the control unit of the private branch exchange. The relevant programs are stored, for example, in a memory module, an EEPROM in this case. A digital signal processor (DSP) having suitable voice recognition software and, optionally, voice recognition hardware is connected to port 21. If the identification is positive, it [emits]relays the signal[for relay] to the private branch exchange via the customary control functions, i.e., either via the line, a V.24 interface, or another

management interface. The [calls]thus[ ]-verified calls are switched from the private branch exchange (PBX) to the interexchange trunk and form an outgoing call. The billing information for person[-]-specific cost assignment is fed directly into the billing system.

In the case of online recognition of the speaker, the call is already set up; however, as [with]in the case of "bugging"[of] a call, the call information is [routed]serially [via]routed through the DSP. The DSP analyzes the speech without interfering with the transmission and relays corresponding information to the private branch exchange or the billing system.

Figure 4A shows an arrangement of control unit IP corresponding to the arrangement of Figure 3A in an exchange. A connection from the subscriber line to an additional line in the public switched telephone network is established via this exchange. Physically and organizationally, the exchange is assigned to the subscriber line; however, it is not necessarily located in its immediate vicinity. Aside from the different physical arrangement of the IP, the access verification is performed here [just]in the same manner as described above. The difference is that no intelligent devices for voice recognition and for speech storage need to be provided on the subscriber side, since these are centrally integrated[centrally] in the exchange.

Figure 4B shows an example for the implementation of access verification by voice recognition in an exchange of a telephone network.

Voice recognition system IP can be implemented in a computer, for example in the form of a plug[-]-in module in the exchange. Calls for which the speaker is to be identified are routed from the exchange [via]through the IP.

Voice recognition is implemented either in dialog form, i.e., an authentication procedure is executed as described above in Figure 3B[above], or else the voice is recognized online. In the latter case, the speech pattern is checked during the conversation in progress and characteristics of the speech of speaking [subscriber]user A are compared with the stored patterns. In this case, the call is tapped, so to speak, by the IP without interfering with it.

One possible structure for the authentication procedure is a dial[-]-in into the DSP of the IP. For this purpose, the telephone channel is routed to an input of the IP. At this point, subscriber A is asked by the software of an intelligent voice response system to state his name or his identifier. After that, he is asked for his password or his personal identification number PIN. The data is compared with the identifier stored in memory, and the speech pattern is compared with the stored patterns either using frequency spectra or speech dynamics. In the dialog form, the implementation of voice recognition is very simple, since the identifier is made up of precisely defined words, which were [entered]previously entered.

After authentication in the IP, the customer is directed to a menu [which]that requests that he enter the desired telephone numbers. These are [received]recorded as in

conventional messaging or voice response systems[and sent into the network], converted into pulse or MFC dialing information, and sent into the network, or they are relayed to the exchange as signals in the format of signaling system No. 7 (Common Channel Number 7, CCS7). The exchange then initiates the connection to subscriber B. The use of CCS7 signals permits faster processing and more features, namely all those implemented in CCS7 and cleared for the IP.

The information concerning the speaker, i.e., the identified reference data record, is sent as control information to the exchange via the CCS7, and generates an alarm in the network management system. The network management system can also generate a corresponding alarm message [via]regarding call data records, so that the billing system also receives appropriate information.

The speaker[-]-identifying data records produced in this way are used for access verification; however, they can also be used for billing a call. The corresponding procedures are described in the flowcharts.

[In]When recognizing continuous speech, the system preferably concentrates on the essential characteristics of the language. To be sure, key words such as "good morning, hello," etc. can be considered in the entry procedure; however, in principle, it is necessary to store speaker[-]-specific characteristics, irrespective of which language and with whom the [subscriber]user is speaking. For this purpose, the algorithm can use static methods[,] such as frequency spectrum analysis, as well as dynamic speech characteristics.

Figure 4C shows an additional example of the method [of]according to the present invention implemented in an exchange. The subscriber unit (subscriber card) of subscriber A recognizes whether the subscriber has provided voice recognition for access verification. The central processing unit CPU of the exchange initiates the appropriate routing [via]through the switching matrix, the actual switching unit. As a result, the call is not routed directly to subscriber B or to the next exchange, but rather it is first routed [via]through an intelligent peripheral IP having a digital signal processor (DSP). The output port of the IP is routed [via]through the switching matrix to subscriber B or to the next exchange.

All control information and, accordingly, also the result of the voice recognition are compared in the exchange having the central processing unit CPU.

The IP [may]can also [contain]include several voice recognition units or DSPs and, thus, analyze several lines simultaneously. The information concerning the usage of the IP and concerning the analytical results is transmitted to the CPU.

Figure 5 shows the implementation of the method [of]according to the present invention in the service control point SCP of an intelligent network.

When [implementation takes place]implemented in the IN, the voice data is routed via an ISDN channel to voice recognition unit $IP_{\perp}$ which is located at the site of the SCP. Control information, for example, whether the calling line [uses]is using voice recognition for [the

control of]monitoring abuse, results [of]from the voice analysis, and the like[,] are then exchanged between the SCP and the service switching point SSP, which is located at the site of the exchange.

[The implementation of]Implementing the method [of]according to the present invention in the centrally structured IN makes [a]it possible to central[implementation of]ly implement voice[-]-based abuse control[possible] over a large network area, i.e., a [large number]plurality of lines. This eliminates the need for expensive software and hardware equipment in the exchanges; only the IN must be adapted. This implementation is, therefore, suitable in particular for cases of low demand or in the introductory phase, i.e., [when the equipping of each exchange]it is not yet worthwhile to equip each exchange.

[Industrial Applicability

]The present invention is suitable, in particular, for operators of communication networks to [enhance]increase the security of voice telephony customers against abuse. Moreover, the present invention is [suitable, in particular,]particularly suitable for operators of private branch exchanges[,] where the problem of unauthorized access is encountered on a regular basis.

Abstract

A method for verifying access authorization for voice telephony in a fixed network line or mobile telephone line, as well as a communications network having such access authorization verification are described. The access authorization is verified by analysis of a voice signal which was entered by the subscriber placing the call, before or during a call in progress. In one variant, the voice signal is entered as a password before the connection is established; in another variant, voice signals are analyzed for voice recognition and subscriber identification, the same voice signals also being transmitted to the person being called, making concealed access verification possible which does not hamper the normal flow of conversation.

09786819

Fig. 1

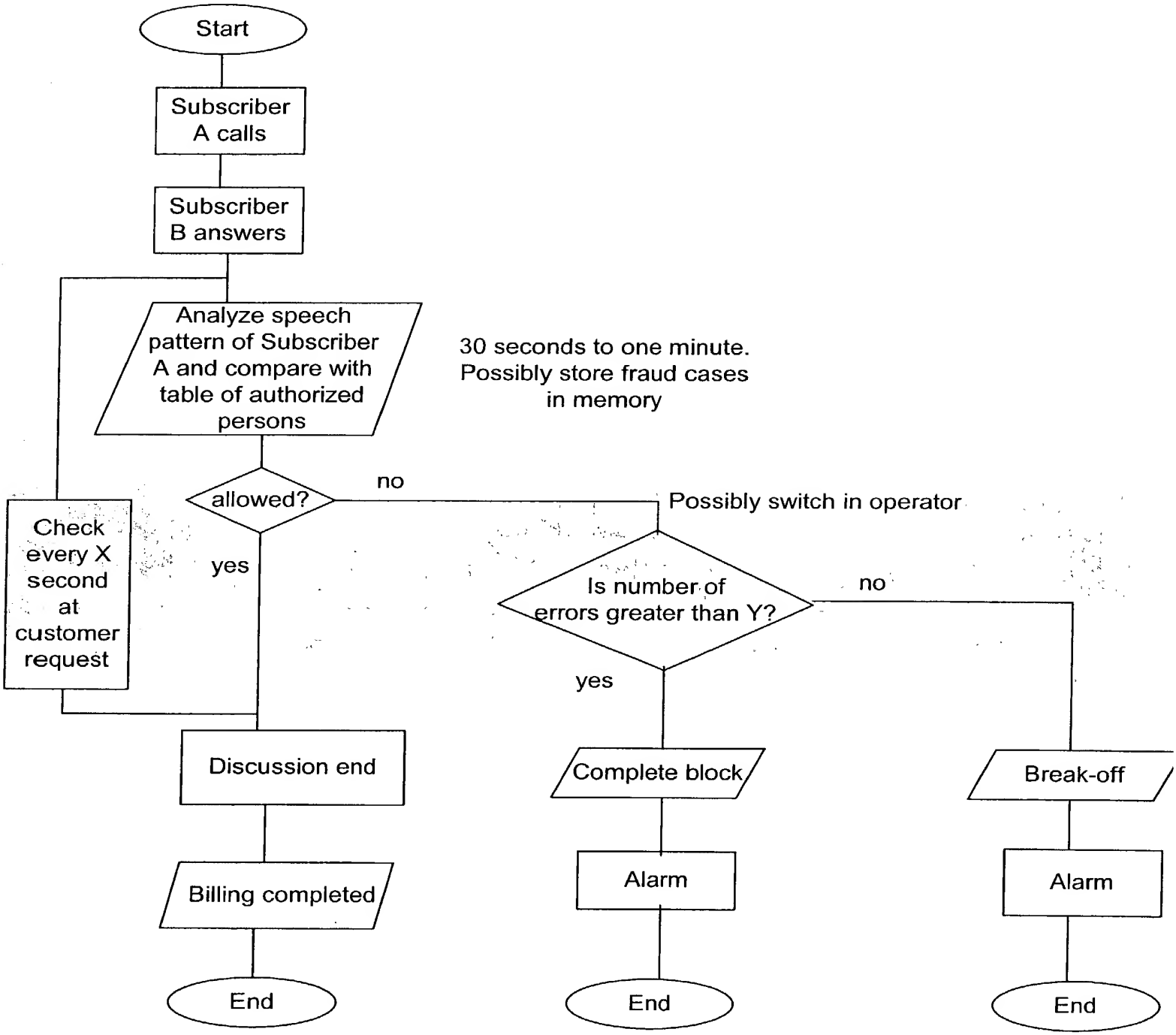
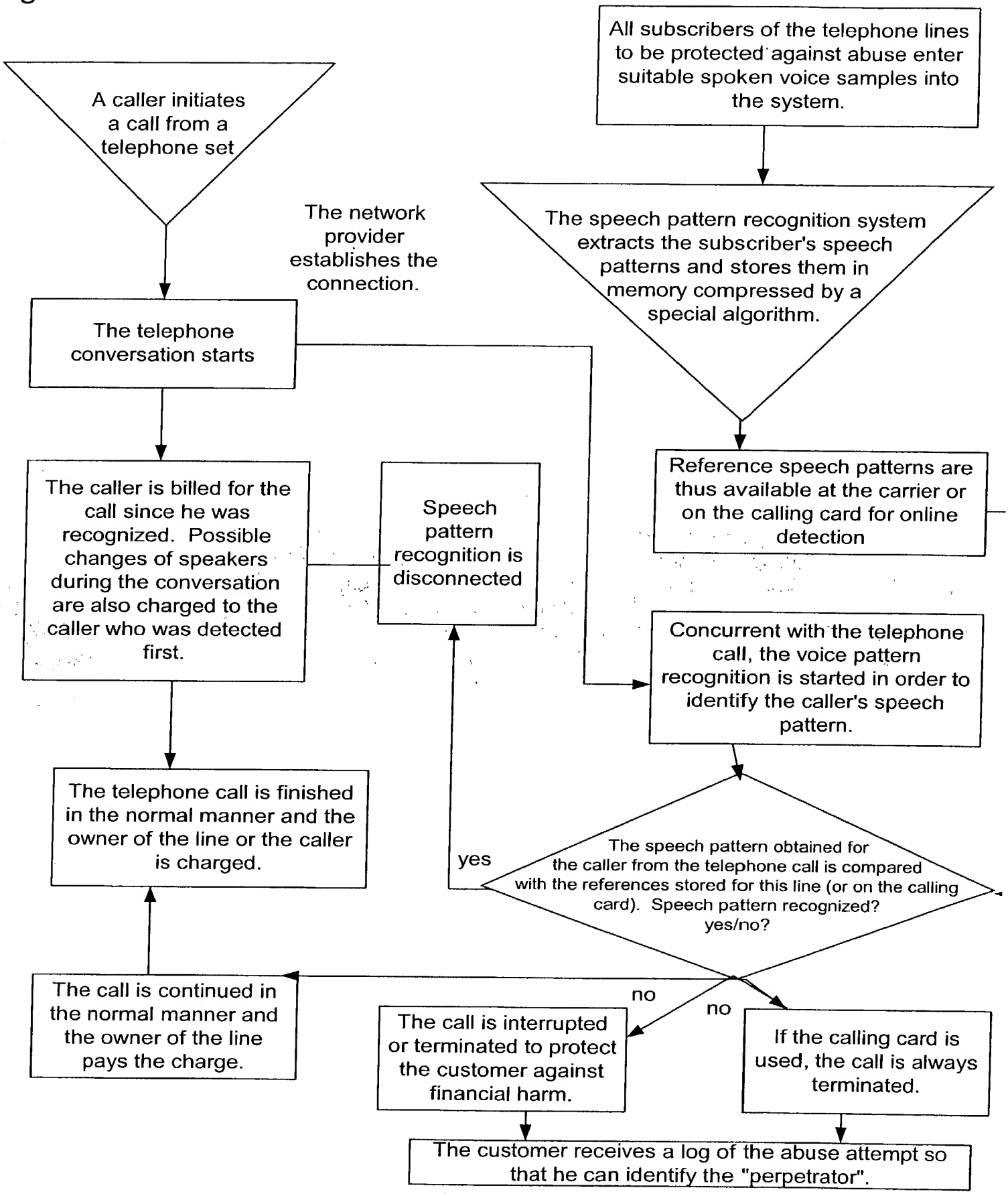


Fig. 2


All subscribers of the telephone lines to be protected against abuse enter suitable spoken voice samples into the system.
A caller initiates a call from a telephone set
The network provider establishes the connection.
The speech pattern recognition system extracts the subscriber's speech patterns and stores them in memory compressed by a special algorithm.
The telephone conversation starts
The caller is billed for the call since he was recognized. Possible changes of speakers during the conversation are also charged to the caller who was detected first.
Speech pattern recognition is disconnected
Reference speech patterns are thus available at the carrier or on the calling card for online detection
Concurrent with the telephone call, the voice pattern recognition is started in order to identify the caller's speech pattern.
The telephone call is finished in the normal manner and the owner of the line or the caller is charged.
yes
The speech pattern obtained for the caller from the telephone call is compared with the references stored for this line (or on the calling card). Speech pattern recognized? yes/no?
The call is continued in the normal manner and the owner of the line pays the charge.
no
no
The call is interrupted or terminated to protect the customer against financial harm.
If the calling card is used, the call is always terminated.
The customer receives a log of the abuse attempt so that he can identify the "perpetrator".

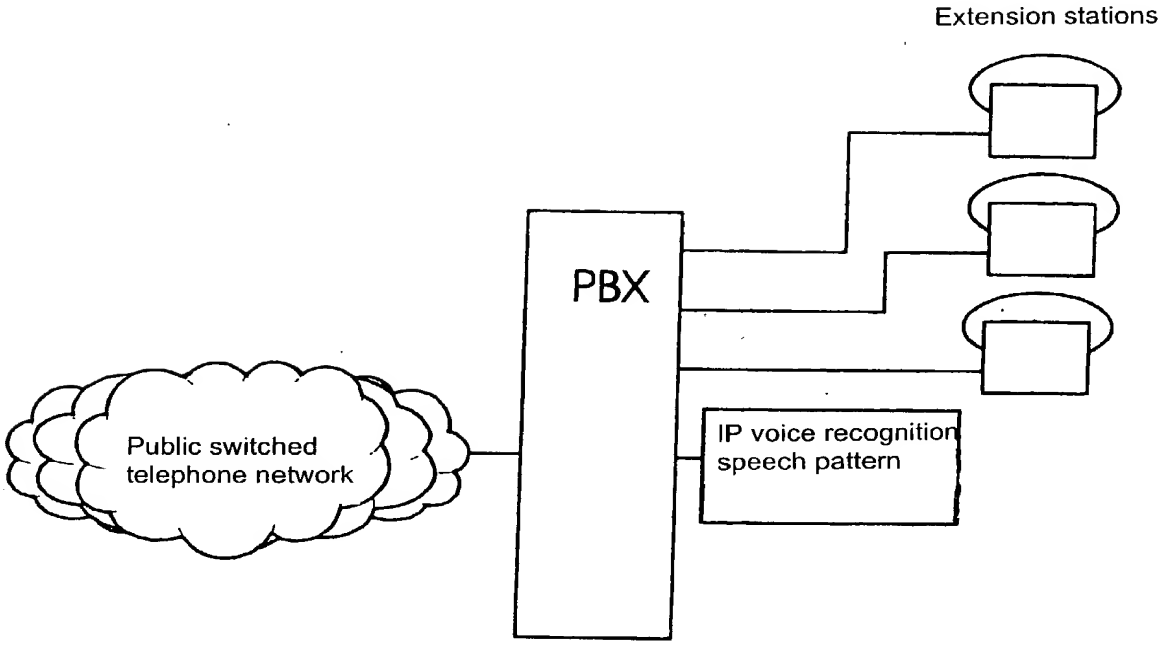

Extension stations
PBX
Public switched telephone network
IP voice recognition speech pattern

Fig. 3a

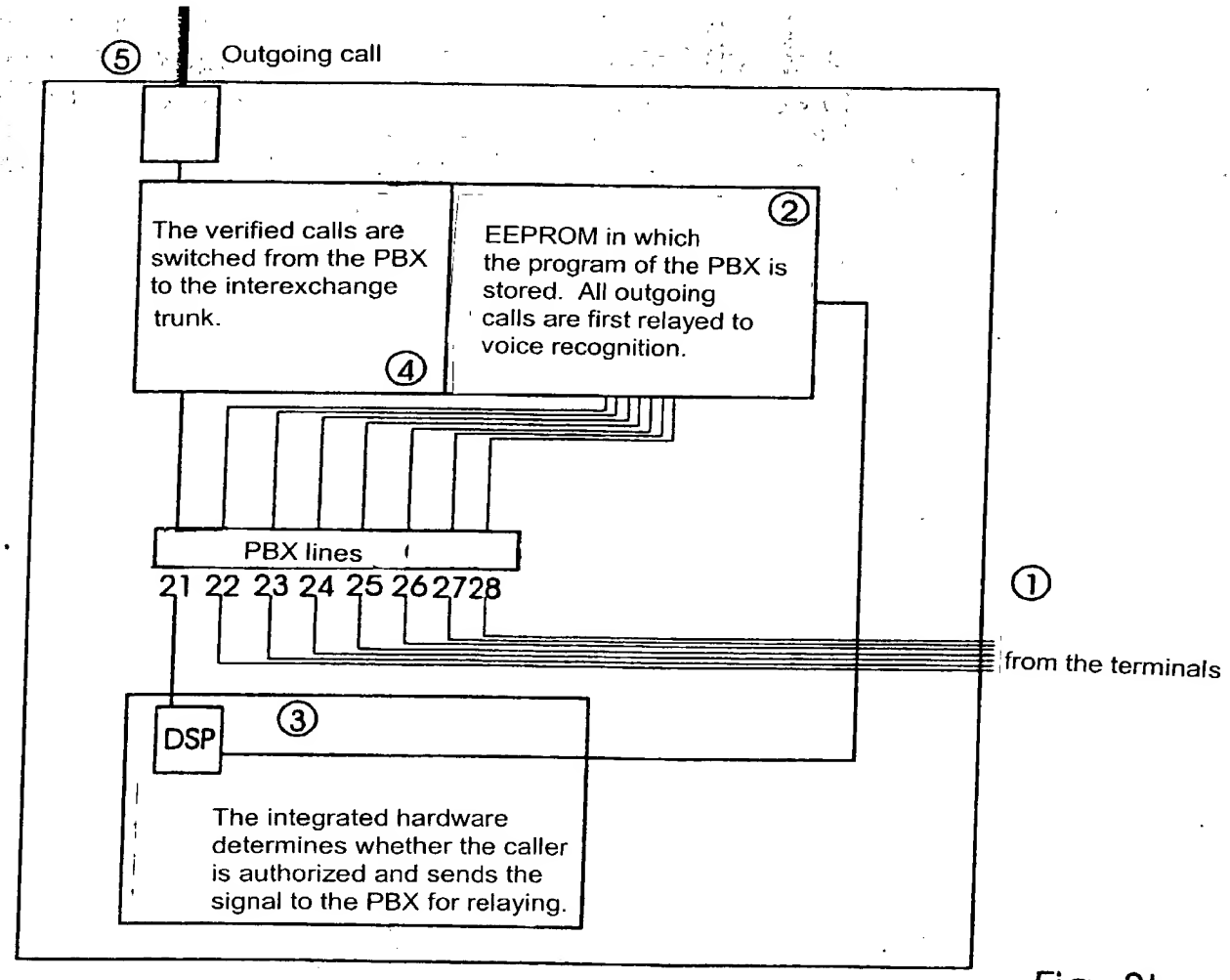

⑤
Outgoing call
The verified calls are switched from the PBX to the interexchange trunk.
④
②
EEPROM in which the program of the PBX is stored. All outgoing calls are first relayed to voice recognition.
PBX lines
21 22 23 24 25 26 27 28
①
from the terminals
DSP
③
The integrated hardware determines whether the caller is authorized and sends the signal to the PBX for relaying.

Fig. 3b

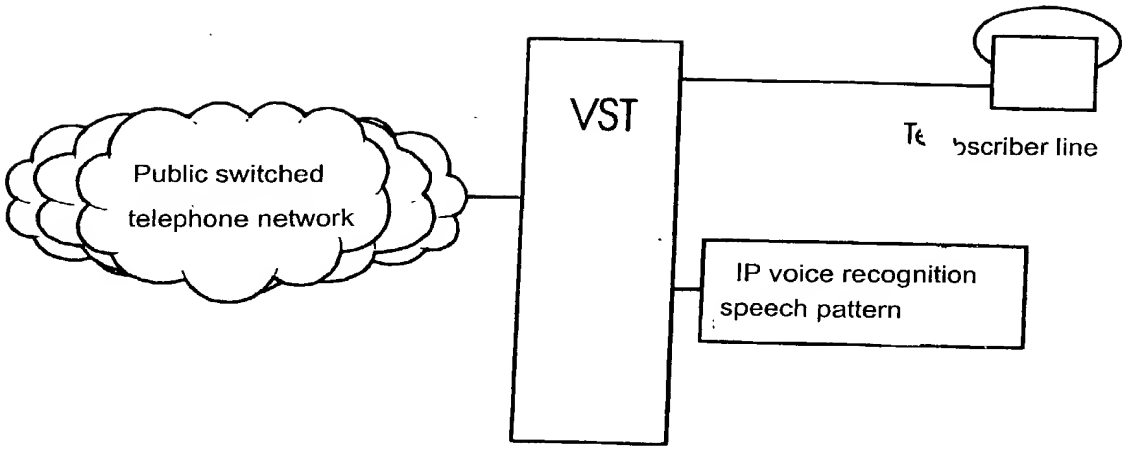

VST
Public switched
telephone network
Te bscriber line
IP voice recognition
speech pattern

Fig. 4a

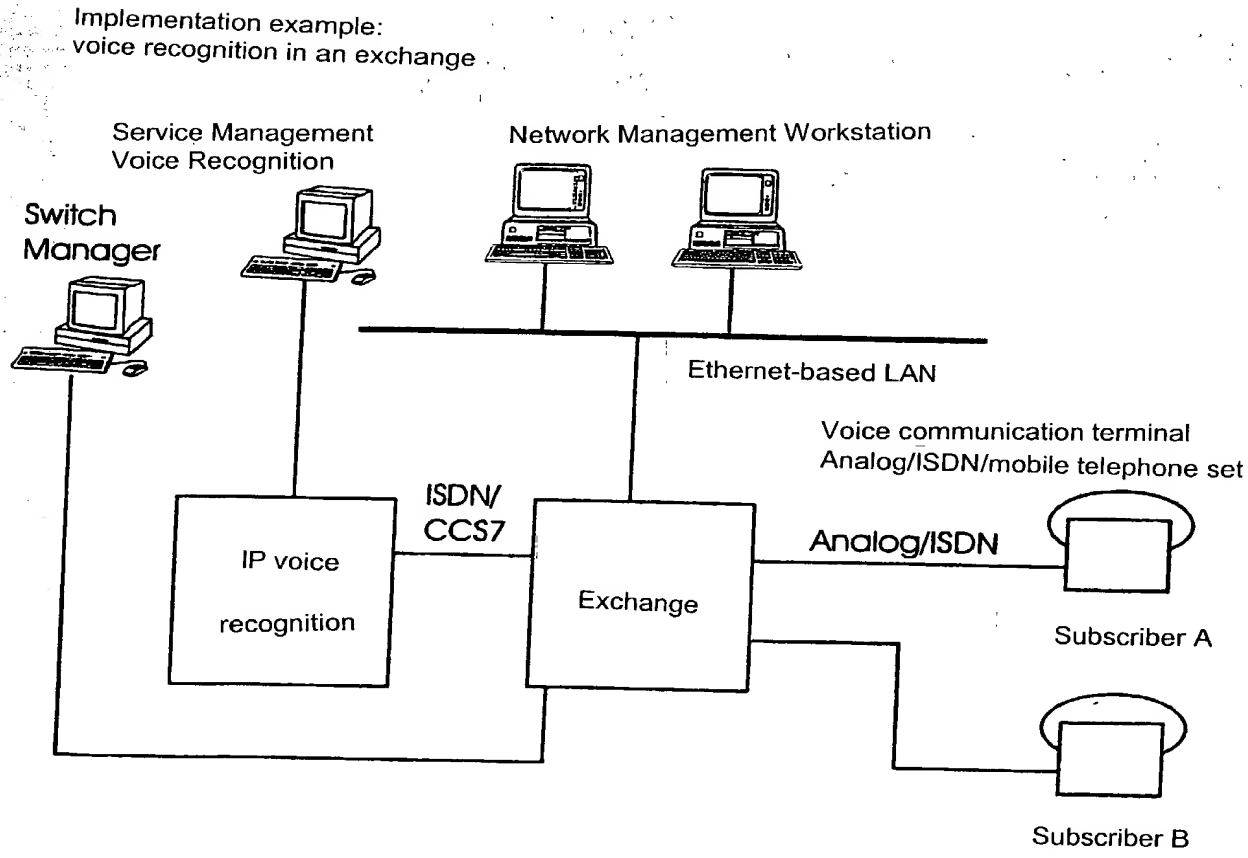

Implementation example:
voice recognition in an exchange
Service Management
Voice Recognition
Network Management Workstation
Switch
Manager
Ethernet-based LAN
Voice communication terminal
Analog/ISDN/mobile telephone set
ISDN/
CCS7
IP voice
recognition
Exchange
Analog/ISDN
Subscriber A
Subscriber B

Fig. 4b

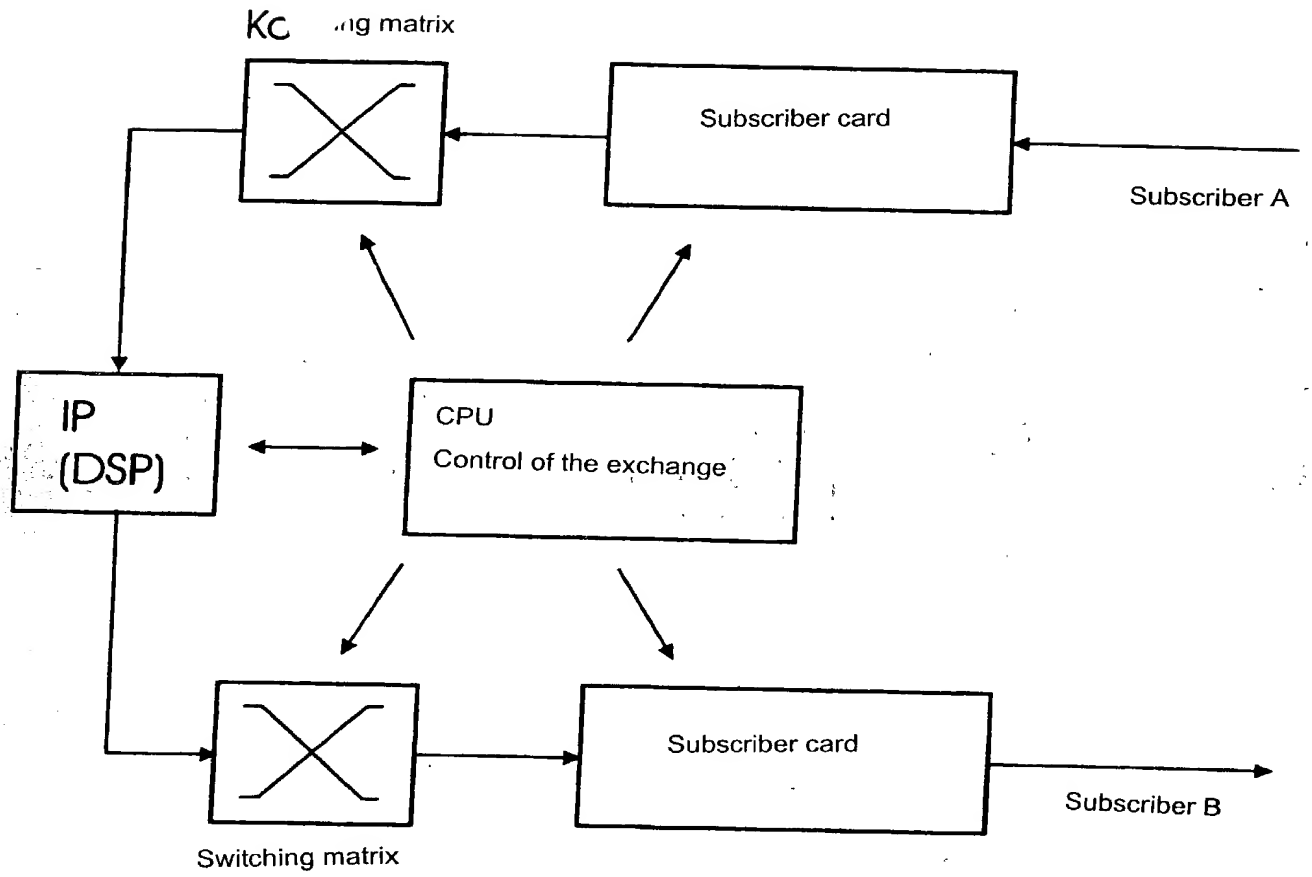

Kc
ıg matrix
Subscriber card
Subscriber A
IP
(DSP)
CPU
Control of the exchange
Subscriber card
Subscriber B
Switching matrix

Fig. 4c

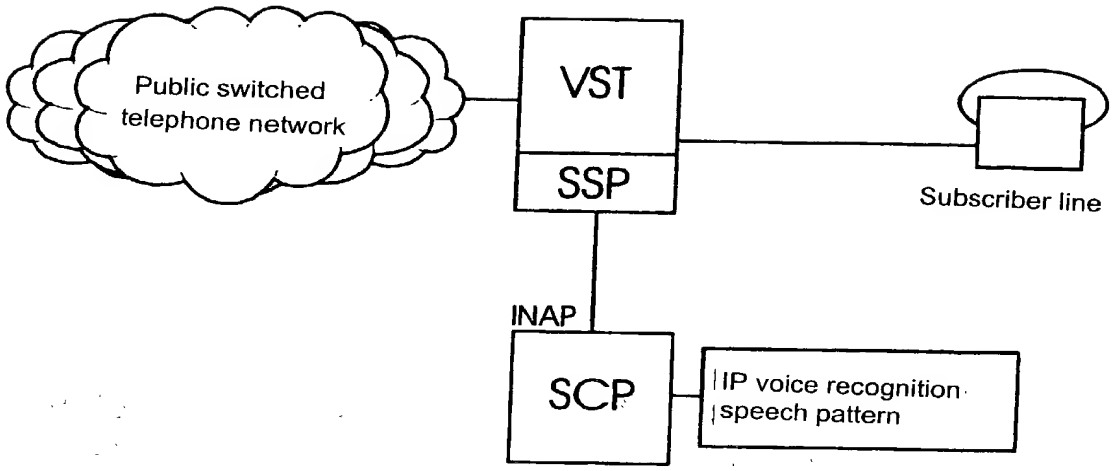

Public switched telephone network
VST
SSP
Subscriber line
INAP
SCP
IP voice recognition
speech pattern

Fig. 5

[2345/147]

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR VERIFYING ACCESS AUTHORIZATION FOR VOICE TELEPHONY IN A FIXED NETWORK LINE OR MOBILE TELEPHONE LINE AS WELL AS A COMMUNICATIONS NETWORK**, the specification of which was filed as International Application No. PCT/EP99/06371 on August 30, 1999, and filed as U.S. application on March 9, 2001 having U.S. Serial No. 09/786,819 for Letters Patent in the U.S.P.T.O.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
198 41 166.9	Fed. Rep. of Germany	9 September, 1998	Yes

Express Mail No. ~~EL799520544S~~ EL327553417US
EL799521844S

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004

CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Axel SUSEN**

Inventor's Signature: _____

Date: 9 July 2002

Residence: Heinrichsallee 66
52062 Aachen
Federal Republic of Germany

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.

Inventor: **Stefan BROCK**

Inventor's Signature: Stefan Brock

Date: 18.7.01

Residence: Hennefer Strasse 6b
53737 Sankt Augustin
Federal Republic of Germany

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.

[2345/147]

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR VERIFYING ACCESS AUTHORIZATION FOR VOICE TELEPHONY IN A FIXED NETWORK LINE OR MOBILE TELEPHONE LINE AS WELL AS A COMMUNICATIONS NETWORK**, the specification of which was filed as International Application No. PCT/EP99/06371 on August 30, 1999, and filed as U.S. application on March 9, 2001 having U.S. Serial No. 09/786,819 for Letters Patent in the U.S.P.T.O.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
198 41 166.9	Fed. Rep. of Germany	9 September, 1998	Yes

EL 799521844S

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004

CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Stefan BROCK**

Inventor's Signature: _____

Date: _____

Residence: Hennefer Strasse 6b
53737 Sankt Augustin
Federal Republic of Germany

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.

Inventor: **Axel SUSEN**

Inventor's Signature: _____

Date: _____

Residence: Heinrichsallee 66
52062 Aachen
Federal Republic of Germany

Citizenship: Federal Republic of Germany

Post Office Address: Same as above.